Comparative Performance Analysis of Network Security Accelerator based on Queuing System

Yeonsang Yun, Seonyoung Lee, Seonkyoung Han, Youngdae Kim and Younggap You

Dept of Information and Communication Engineering, Chungbuk Nat'l University, Chongju City, Kcrea 361-763
Tel : +82-43-271-2480 Fax : +82-43-271-2480 E-mail: ysyun@hbt.chungbuk.ac.kr

Abstract:

This paper presents a comparative performance analysis of a network accelerator model based on M/M/1 queuing system. It assumes the 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 only 15% differences with respect to actual measurements on field traffic for 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: Network security accelerator/Queuing modeling/Poisson distribution

1. INTRODUCTION

Security protocols such as IPSec or SSL take crucial roles in communication network as network security becomes troublesome issues. Implementation of IPSec protocols demands a substantial amount of CPU loads to process operating systems software. It is reported that this load consumes more than 95% of CPU resources for security application[1]. Security accelerators become attractive solutions alleviating this CPU overload problem[2]. Network security accelerators process cryptic commands on behalf of its CPU, and thereby distributes overall system loads.

Network security accelerators address mostly chip level performance within a system. BCM5820 model of Broadcom, for example, claims the maximum performance of 300Mbps for 3DES+SHA operations[11]. Actual performance of the network security accelerator within a network computer yields at most 50% of the claimed performance[3]; this figure is obtained under the best network specification and for the network bandwidth of 1Gbps. It is extremely difficult to achieve the claimed performance of network security accelerators. Realistic performance analysis of network environment gives a way to get some reasonable network security accelerator specification and operation modes.

This paper proposes a comprehensive performance analysis model of network computers arming with network security accelerators. Conventional performance analysis employes either physical measurements with some equipments or simulation with system behavioral modeling. The proposed approach is based on modeling of target systems and simulation of their behavior. Recently simulation results are found similar to those obtained through physical measurements[4]. The proposed model employs a queuing model, and evaluates with a commercial simulation tool Anylogic- 4.5. Anylogic4.5 supports test environment handling 50,000 objects on a medium size workstation (PIV 1.7GHz, 512MB RAM)[5,6]. Section II of this paper presents performance analysis overview with modeling and the proposed analysis model. Section III delivers simulation results, and finally Section IV concludes with some evaluation.

2. THE PROPOSED PERFORMANCE ANALYSIS MODEL

The proposed performance analysis model comprises a queuing model of a network computer equipped with a network security accelerator. Components of the proposed performance analysis model are explained shortly.

2.1. Queuing Model of Network Computers with network security accelerator

A M/M/1 queuing system is illustrated in Figure 1. The M/M/1 queuing system features a service request arrival rate (λ) and a processing rate (μ; processing time:$1/\mu$) to compute average waiting time with the equation (1). The response time is the sum of the waiting time and the processing time shown in (2).

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

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

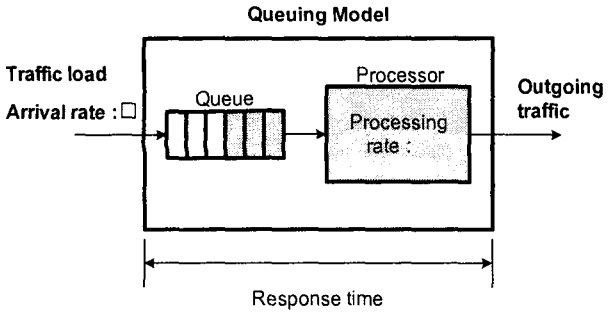

Fig. 1. M/M/1 queuing modeling

Most commercial network security accelerators are attached to a network computer through a PCI interface as illustrated in Figure 2. The CPU fetches an instruction from its main memory and then executes it. The CPU controls its network interface or network security accelerator by instructions from main memory. Operating system determines the types of instructions to be executed. Operating system, main memory and CPU are characterized by three system parameters affecting the operation of a network security accelerator. Network computer modeling includes the three parameters in addition to the performance of the network security accelerator.

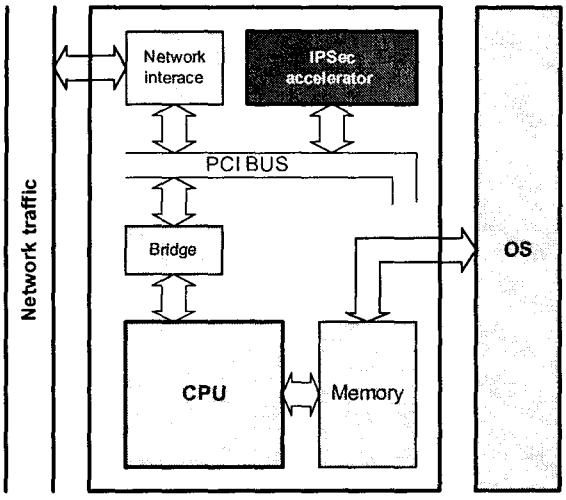

Fig. 2. System model of a network computer with network security accelerator

An M/M/1 queuing model of a network processor with a network security accelerator is illustrated in Figure 3. Virtual traffic loads replace the input service request during the analysis with the model. The queue of the proposed M/M/1 system represents input buffers of the network interface within a network computer with IPSec. The queue receives the virtual traffic load. Network security accelerator corresponds to the processor of the M/M/1 system with the processing time of $1/\mu$. The decoding delay represents the time consumed by other components such as PCI bus, CPU, main memory, operating system between the network traffic input and network security accelerator.

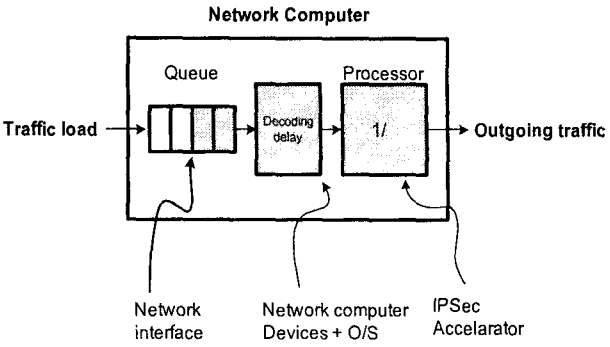

Fig. 3. Queuing model of a network computer with network security accelerator

2.2. Traffic Load

A network security accelerator reduces computation loads due to operating system or cryptic application softwares handling IPSec protocol. Instructions for operating system or security application are the command input of the network security accelerator. Operating system may issue, for example, a simple command "CryptoAPI" to process 3DESS+SHA using the network security accelerator. Input packets from its network can activates the execution of operating system commands.

The proposed performance analysis model employs a traffic load with Poisson distribution. Poisson distribution is a reasonable traffic behavior model representing network traffic. Paxon and Floyd showed that actual network traffic differs from Poisson distribution in 1995[8]. But they proved the network traffic of session arrivals has Poisson distribution for the time period of 10^3 seconds. Session arrival traffic is observed when a client tries an initial connection to a server. The network traffic under IPSec protocol looks very similar to the session arrival traffic due to the security association of initialization messages. Poisson distribution is a promising model representing the traffic load of IPSec.

Explosive increase in network users since Paxson and Floyd investigation is another reason to support the Poisson distribution to model network traffic. The number of user increase is illustrated in Figure 4. Session arrival time period 10^3 to have Poisson distribution should be revised to meet current network traffic statistics. The number of users in 2002 increases 78 times since 1995, and the number of server increases very slowly. The ratio of a user to host servers decreases from 10.11% in 1995 to 2.84% in 2002.

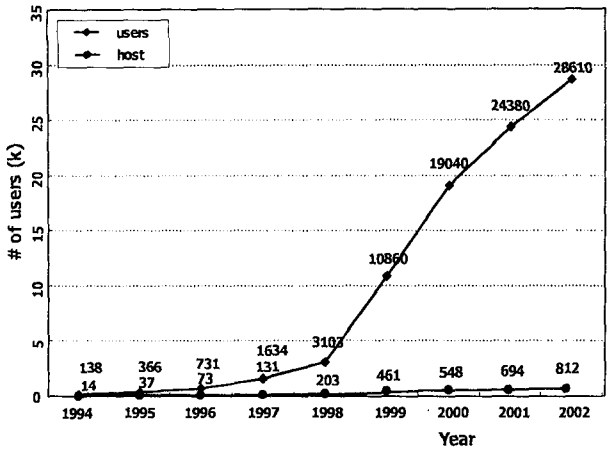

Fig. 4. Internet subscribers[9]

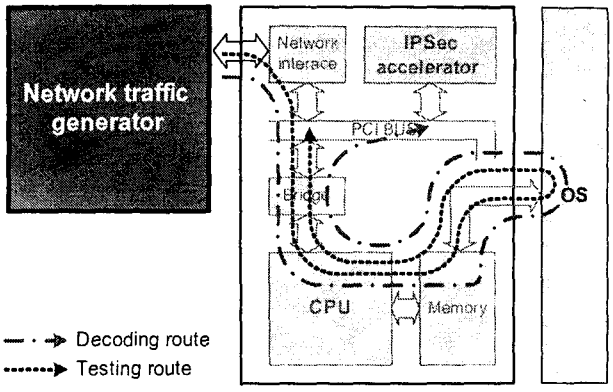

Fig. 5. Decoding and test route of a network computer with an network security accelerator

It means the number of clients increases explosively with respect to the number of host servers. The input traffic increase of a host server can be calculated with the following equation (3).

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

Network bandwidth to clients is another factor supporting the Poisson distribution. The network bandwidth of 2002 increases at least 20 times larger than that of 1995. Reflecting the foregoing facts of UHR represented in the equation (3), network bandwidth increase, the time period counting network traffic arrivals to justify the Poisson distribution of Paxson and Floyd has reduced by 5000 times compared to that of 1995. The time period of 10^3 seconds for Poisson distribution reduces below 1 second in 2002. This paper takes 10 seconds for the time period to use the Poisson distribution reflecting the worst case guard bands.

2.3. Input Parameter

The proposed performance analysis model features three input parameters of λ, $1/\mu$, decoding delay: λ is the arrival rate of network input packets for the simulation tool Anylogic 4.5; and $1/\mu$ is the processing time. The best performance data announced in data sheets are used for the processing time of a network security accelerator. A processing rate(μ) of 300Mbps corresponds to the 3.3nsec of processing time($1/\mu$).

The decoding delay is a parameter introduced in this paper in addition to the conventional λ, μ of a M/M/1 system. It represents the time for traveling the decoding route. Traveling route of a network packet and operation commands between input and network security accelerator is shown in Figure 5. Decoding delay may vary along the performance variables such as of hardware of network computer and operating systems.

A test route is used to compute decoding delay. A test program has been devised to get decoding delay of a network computer. The test apply packets along the test route, process the packets, and moves the processed packets to the network interface. The time period of this entire test process constitutes the decoding delay. A network traffic generator issues packets to the network computer. The issued packets finally arrive at the network interface through the test route. The modeling parameters are the basis of decoding delay calculation. The test program execution is illustrated in Figure 6 and Figure 7.

3. SIMULATION RESULTS

A simulation based on the proposed performance analysis model evaluates a network computer comprising commercial network security accelerator BCM5820. The results are compared to physical performance measurements on a network computer with BCM5820 network security accelerator[3].

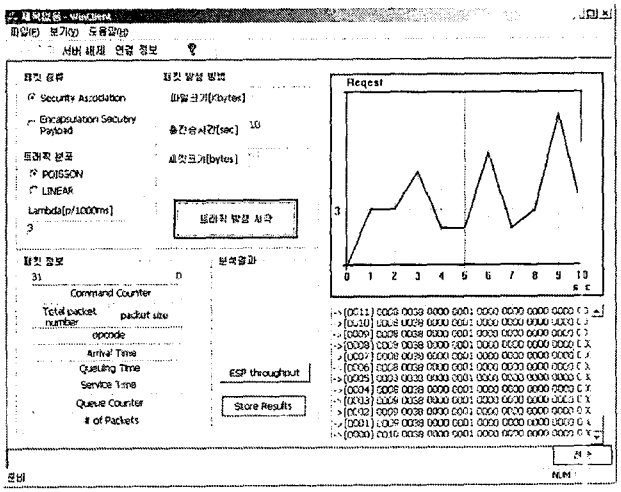

Fig. 6. Test program - traffic generator

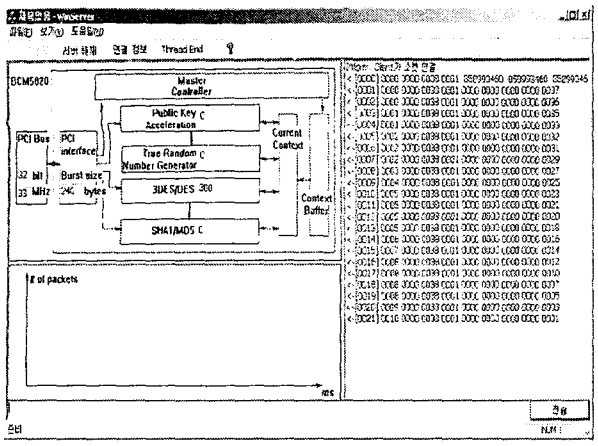

Fig. 7. test program - test route

3.1. Parameter Values

Parameter values of the proposed performance analysis model reflects characteristics of currently used network computers. Table 1 shows the listed values. The simulation analyzes the function of 3DES+SHA running on the BCM5820 network security accelerator. The processing rate(μ) of BCM5820 applicable to the 3DES+SHA function is 300Mbps, corresponding processing time($1/\mu$) of 3.3nsec/bit. Arrival rate λ can be generated using the function DistriPossion.sample($1/\lambda$) supported by Anylogic-4.5. Full network traffic load prevents idle processor states. The actual value of the arrival rate(λ) is 0.4msec equivalent to the network bandwidth of 1Gbps. Repeated simulation runs using the proposed test program yield an average decoding delay of 0.5msec. The test program is executed using a network computer specified in Table 1 to compare with the Miltchev's measurement results. Table 2 lists the test environment used in Miltchev's performance evaluation.

Table 1 Test program operation conditions to get decoding delay

Hardware	CPU	1GHz Intel P3 processor	decoding delay : 0.5msec
	Memory	256MB PC133 SDRAM	
	Hard drive	40GB	
OS	OS	Windows2000 PRO	

Table 2 **Test environment of Miltchev's work[3]**

Network	Bandwidth	1Gbps(host-to-host)
Accelerator	network security accelerator	BCM5820
Hardware	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
OS	OS	OpenBSD 3.0

3.2. Simulation Results

Throughput of the network security accelerator is a target performance measure to be obtained through simulation based on the proposed performance analysis model, which is represented in Mbps with respect to a set of different packet sizes. Figure 8 shows two stages of a simulation using Anylogic4.5 distributing heavy load during the simulation run. Outputs from Simulation 1 are used as input parameter values of Simulation 2. Simulation 1 evaluates processing time when 50kbytes of data are sent in different packet sizes specified in Table 3. Simulation 1 yields the total decoding delay of the network security accelerator. The sum of this delay and $1/\mu$ is the input value of overall processing time for Simulation 2.

Table 3 lists the overall processing time from the simulation run for the file of 50kbytes with respect to different packet sizes. The processing speed of 3DES+SHA of BCM5820 is assumed 300Mbps(μ), and the average time to process the 50kbytes is found 1.333msec. The number of 64byte packets is 782 for the 50kbyte file. The number of decoding and decoding time decrease as the packet size increases.

Simulation time for each case of packet sizes (64~65546byte) is 100 seconds to meet the minimum time interval of 10 seconds to secure Poisson distribution on network traffic. An average value for a case is obtained through 100 repeated simulation runs.

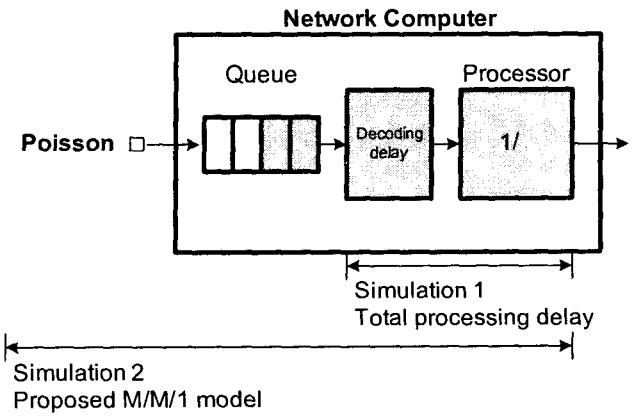

Fig. 8. Simulation stages of the proposed performance analysis model

A comparison between the results obtained through the simulation and the Miltchev's measurements are illustrated in Figure 9. Average differences between the two evaluations are less than 15.4%. For packet sizes smaller than 8192 bytes yield average differences lower than 13.3%. Note that the maximum packet size of the message transmission unit is 1500 bytes, and the most frequently used packet sizes for media streaming units is 820 bytes[10].

Table 3 Overall processing time for packet sizes(unit : 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

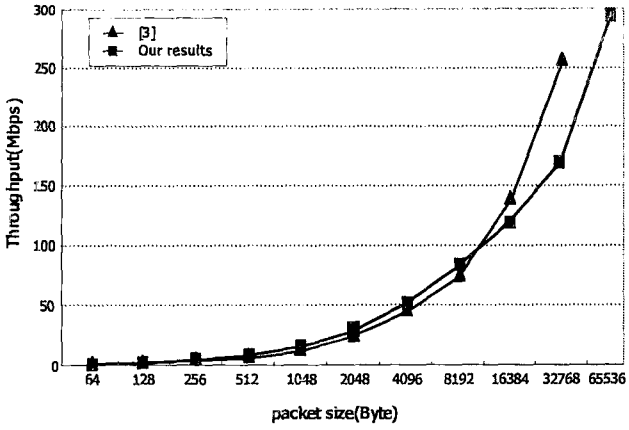

Fig. 9. Simulation results

4. CONCLUSION

This comparative analysis between simulation and measurements is to establish a realistic low cost performance evaluation method through simulation. The proposed performance analysis model yields viable evaluation results close to physical measurements: only 15% average difference is observed. This small difference means the proposed queuing model reflects realistic traffic loads and parameters of a network computer equipped with a network security accelerator. It also allows a network computer performance variation through a decoding delay estimation. A test program has been devised to get the decoding delay of a target computer. The simulation results verify the accuracy of the decoding delay values. Conventional evaluation approaches rely on costly measurements using expensive equipments. The proposed model reduces the time and expenses of performance evaluation of network computers with a network security accelerator. The performance model can be used to span design spaces of network computers comprising IPSec acceleration delivering the maximum performance.

References

[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 secutity protocols," *In Proceedings of USENIX Annual Technical Conf.*, Freenix Track, pp. 41-48, June 2002.

[4] T. 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, "Systems 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*, www.xjtek.com.

[7] L. Kleinrock, *Queuing Systems, Volume I: Theory*, John Wiley, 1975.

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

[9] National Computerization Agency, *Information-oriented White Paper 2002*, www.nca.or.kr/data_pdf/b2002eng.pdf

[10] 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.

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