기가비트 네트워크 지원을 위한 TOE 기반 IPSec 시스템

신치훈[*,**], 김선욱[**], 박 경[**], 김성운[**]
과학기술연합대학원대학교(UST) 컴퓨터 및 소프트웨어공학과[*]
한국전자통신연구원(ETRI) 서버플랫폼연구팀[**]

The IPSec Systems on TOE for Gigabit Network

Chi Hoon Shin[*,**], Sun Wook Kim[**], Kyoung Park[**], and Sung Woon Kim[**]
[*]*Computer S/W Engineering in University of Science and Technology,*
[**]*Server Platform Research Team in Electronics and Telecommunications Research Institute,*
E-mail: cshin@etri.re.kr

Abstract -- This paper describes the designs and the implementations of two H/W IPSec Systems, look-aside and inline, on TOE (Transport Offloading Engine). These systems aim for guaranteeing the security of datagram networks while preserving the bandwidth of gigabit networks. The TOE offloads a host CPU from network burdens, so that it makes the gigabit wire speed possible, and then deeper level security architecture of the IPSec guarantees the security of gigabit service network dominated by datagram packets. The focus of this paper is to minimize the TOE's performance degradation caused by the computation-oriented IPSec. The look-aside IPSec system provides a significant improvement in the CPU offload of the IPSec cryptography loads. However, the inline system completely offloads the host CPU from whole IPSec loads, providing significant additional cost saving compared to the look-aside system. In this paper, the implementations of TOE cards including commercial IPSec processors are presented. As the result of performance evaluation with the protocol analyzer, we can get the fact that the inline IPSec system is 8 times faster than the S/W system and 2 times faster than the look-aside system.

I. Introduction

네트워크 서비스 환경이 점차 기가비트 환경으로 발전해 가고[1][2][12] 그 사용 방식은 대량의 단발성 datagram 중심으로 변해가고 있다[2]. 환경이 변해감에 따라 기가비트 네트워크의 wire speed를 지원하기 위한 서버의 시스템구조의 개선책과 datagram이 주도하는 새로운 사용 방식에 대응할 수 있는 security 체계의 필요성이 대두되고 있다[13].

기가비트 서비스 네트워크 환경으로의 발전해 나가기 위해서는 넘어서야 할 장애물이 있다. 그것은 네트워크 대역폭의 발전 속도가 프로세서의 발전 속도를 초과하고 있는 현상이다. 인터넷 사용자의 기하급수적인 증가와 광대역가입자망의 보급에 따라서 네트워크 트래픽이 증가하고 서비스가 고품질화에 따라서 요구되는 대역폭이 커졌다. 이러한 요구로 생겨난 네트워크 성능 향상의 노력이 결국 CPU 발전 속도보다 네트워크 발전 속도를 더욱 빠르게 만드는 요인이 되었다[2]. 하나의 프로세서만으로는 기가비트 네트워크 서비스가 요하는 성능을 만족시키기 어렵게 된 것이다[6].

또한 새로운 security의 체계를 도입하는 문제도 간단한 일이 아니다. datagram은 비 연결지향적 이므로 SSL (Secure Socket Layer) 같은 transport layer 이상의 연결 지향적인 보안 수단으로는 datagram 중심의 트래픽에 효과적으로 대처 할 수 없다. 서버는 network layer 이하의 보안구조를 이용해 datagram의 안전을 보장해야 한다[3][4]. 하지만 이 방법들은 하위 layer 에서 호스트로 복잡한 계산을 요청하게 되므로 대량의 datagram 처리시 서버시스템이 기가비트 wire speed를 내지 못하게 하는 또 하나의 걸림돌로 작용할 수 있다.

따라서 기가비트 네트워크 서버시스템에는 다음과 같은 요구사항들이 필요하다. 첫째, network load를 전담할 수 있는 별도의 프로세서파워가 필요하다. 둘째, 비연결지향적인 datagram을 보호할 수 있는 security 체계가 필요하다. 마지막으로 이 security 체계는 기가비트 wire performance를 보장하기 위해 overhead가 적고 스피드가 빨라야 한다.

본 논문에서는 이러한 요구사항들을 해결할 수 있는 TOE기반 H/W IPSec 시스템에 대해 알아보고 그 구현으로서 Hifn IPSec on LATONA -Advanced TOE를 제안한다. 마지막으로 LATONA 기반 S/W only, look-aside, inline IPSec system 간의 성능비교를 통해 어떤 방식이 기가비트 서버 네트워크 환경에 적합한지를 검증하는 비교 데이터를 제시하였다.

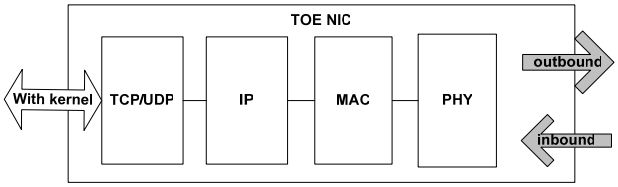

그림 1. Transport Offload Engine (TOE)

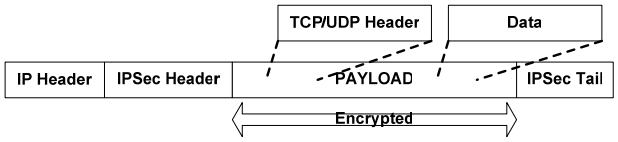

그림 2. IPSec Packet

II. H/W IPSec on TOE

Transport Offload Engine (TOE)과 H/W로 구현된 IP Security (IPSec)의 조합은 기가비트 네트워크 서버 시스템의 요구사항들을 만족시킬 수 있다.

1. Transport Offload Engine (TOE): TOE 는 interrupt overhead, memory transfer 등으로 인해 야기 되었던 딜레이를 없앨 수 있다. 그림 1 처럼 TOE 는 네트워크 stack 을 하드웨어로 구현하여 network load 를 메인 프로세서가 아닌 NIC (Network Interface Card)에 내려 별도의 프로세서에서 담당하게 하는 구조이기 때문이다. 이 방식은 Network load 를 host CPU 로부터 독립시켜 TOE 프로세서가 기가비트 네트워크의 speed 를 보장하는 것에만 집중 할 수 있게 해준다[2].

2. IP Security (IPSec): IPSec은 datagram 중심의 네트워크를 위한 근본적인 보안수단이 될 수 있다. 그림 2 에서처럼 IPSec은 IP layer에서 직접 암/복호화와 패킷인증 등을 처리하므로 어떤 transport layer 프로토콜이 오든 상관하지 않기 때문이다[3][4][5][7]. 그러나 IPSec은 근본적으로 계산지향적인 프로토콜로서 소프트웨어로 구현될 경우 매우 느릴 수 밖에 없다. 더구나 host는 IPSec 이외에 여러 보안 관련 처리도 동시에 행해야 한다. 때문에 IPSec은 서버의 성능에 심각한 딜레이를 야기할 수 있다. 따라서 IPSec의 계산지향적인 부분들은 호스트로부터 독립시켜 H/W로 구현 되어야 한다[5].

3. H/W IPSec on TOE: TOE는 gigabit network speed 를 보장하고 동시에 H/W IPSec가 gigabit speed를 해치지 않고 datagram의 보안을 책임질 수 있어 H/W IPSec on TOE는 기가비트서비스 네트워크를 위한 최적의 솔루션이 될 수 있다. 이 시스템은 다음과 같은 두 가지 방식으로 구현될 수 있다. 하나는 IPSec의 일부분만 H/W로 구현하는 **look-aside 방식**이다. 이 방식은 IPSec의 기능 중 일부분을 H/W로 구성한다. 하지만 이 방식은 host 버스를 통해 패킷 데이터를 주고 받으므로 버스오버헤드를 가지고 있고 디자인이 복잡하다는 단점이 있다. 다른 하나는 IPSec의 모든 기능을 H/W로 구현하는 **inline IPSec 방식**이다. In-line 구조는 look-aside 구조가 가지는 단점 해결을 위해 제안되었다[5]. Inline구조는 네트워크 stack으로부터 독립된 H/W IPSec 시스템을 구성

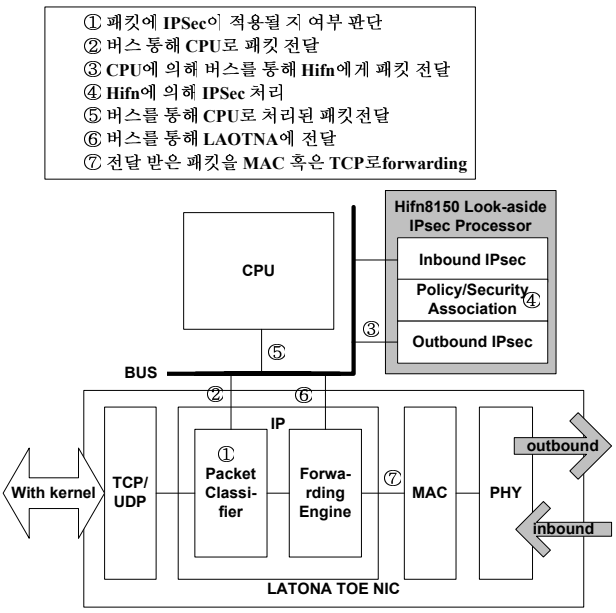

그림 3. Look-aside IPSec의 구조

하여 look-aside의 단점들을 극복하고 있다.

TOE 기반의 look-aside, inline방식은 H/W IPSec의 처리성능을 이용하여 datagram security에 대해 근본적으로 대처하면서 TOE에 의해 지원되는 기가비트 네트워크의 wire speed를 손실 없이 보장할 수 있다.

III. Hifn IPSec on LATONA -Advanced TOE

본 논문에서는 H/W IPSec on TOE의 최적화된 구현으로서 ETRI에서 개발된 LATONA (Leading Architecture for TCP Offloading & Network Acceleration)[2] TOE에 Hifn사의 IPSec 프로세서[8]를 접목한 시스템을 제안한다. Hifn 프로세서는 H/W IPSec core를 사용해 IPSec의 복잡도로 인한 성능감소를 해결하고 LATONA는 H/W IPSec에 적합한 full offload의 독립된 NIC으로써 기가비트 서비스 네트워크의 성능을 보장해 주는 여러 가지 feature들을 가지고 있다.

LATONA는 full offload 방식이며 900Mbps 의 sending, 200Kpps Receiving, 10K connection 의 성능을 가지고 있고 BSD 소켓 호환성제공, zero-copy 기술, 소형 패킷 처리성능 최적화 기술, PCI-Express host bus기술이 접목된 진보된 형태의 TOE이며 특히 대량의 단발성 datagram을 처리할 수 있도록 설계되어있다[2]. 그리고 IPSec 프로세서로는 look-aside 방식의 hifn8150 과 inline 방식의 Hifn8300 을 사용하였다[8].

***1. Hifn Look aside IPSec on LATONA*:** Hifn8150 look-aside IPSec 프로세서는 IPSec 의 cryptography 를 담당하는 주요 부분을 H/W 로 구현한 방식이다. 계산비중이 높은 부분을 H/W 으로 구현하여 성능을 끌어내는 것이다. 그림 3 은 Hifn8150 look-aside 의 Outbound packet 의 처리과정을 보여주는 그림이다. 이 구조에서는 입력된 패킷이 LATONA 를 통해서 메모리에 저장되고 만약 보

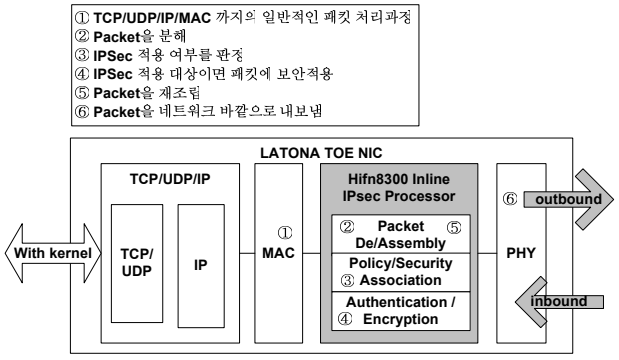

그림 4. Inline IPSec의 구조

안이 필요하다면, hifn 프로세서에 의해서 처리된 다음, 다시 메모리에 저장되고, 네트워크바깥으로 출력된다. 이 방법은 S/W IPSec 보다 빠른 보안 처리가 가능하다.

2. Hifn Inline IPSec on LATONA: Hifn8300 inline 프로세서는 LATONA 의 PHY (Physical Layer)와 MAC (Media Access Control Layer) 사이에 IPSec 프로세서를 삽입되는 형태로 구현된다. 그림 4 는 hifn8300 inline IPSec 의 구성을 나타낸 것이다. Look-aside 방식이 IPSec 관련 기능의 일부분 만을 전용프로세서에 할당했다면 이 방식에서는 IPSec 과 관련된 모든 기능을 전용프로세서 에서 해결한다. 아웃바운드 패킷을 예를 들어보자. 커널을 통해 LATONA 에 전달된 payload 는 TCP/UDP/IP, MAC 까지 IPSec 의 아무런 영향을 받지 않고 패킷화 된다. 이 패킷은 PHY 의 앞에 위치한 IPSec 프로세서를 거치면서 비로소 IPSec 의 적용을 받게 된다. 이를 위해 hifn8300 프로세서는 패킷 분해, 재구성 기능을 가지고 있다.

이러한 방식은 인터페이스가 단순해 디자인비용과 Time To Market 을 줄일 수 있고 버스가 가지는 오버헤드와 병목현상을 없앨 수 있다. 이 프로세서는 네트워크 측에서 볼 때는 마치 MAC 처럼 보이고 호스트 측에서 볼 때는 PHY 처럼 보이게 되는 투명한 구조이다[5]. 따라서 기존의 TOE 디자이너는 IPSec 프로세서에 대해 신경 쓸 필요가 없다. 또한 이 구조는 네트워크 프로세서와 보안 프로세서 사이에 복잡한 데이터 전송과 반송 과정이 필요 없고, TOE 에서는 IPSec 장치에 의해 인증해석과 복호화가 이미 완료된 패킷만을 처리하므로 Look-aside 처럼 full duplex bus 를 통한 통신이 필요 없다.

3. LATONA IPSec Control S/W: Hifn 프로세서를 제어하기 위해서는 컨트롤 프로그램이 필요하다. 사용자가 Hifn IPSec 프로세서를 동작을 위해서는 펌웨어 다운로드와 GMAC 등 LATONA 와의 인터페이스를 초기 화를 수행하고 테이블을 설정해야 한다. 제어프로그램이 Hifn 프로세서와의 통신을 위해 사용하는 PPCI 는 고유의 프로토콜이며 Hifn 프로세서는 PPCI 타입의 이더넷 패킷을 통해 유저영역으로부터 모든 설정정보를 받아들인다. Hifn 은 PPCI 패킷 받아 해석하여 설정을 적용한다. 구체적인 구성과 동작 순서를 그림 5 에 나타내었다.

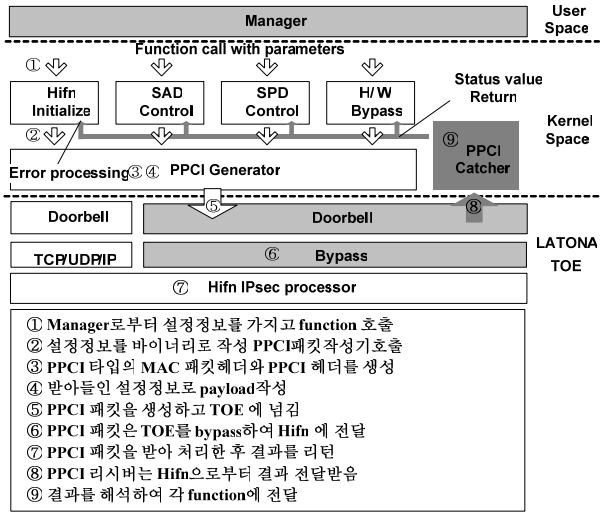

그림 5. Inline IPSec system management system

IV. Performance Evaluation

이 장에서는 LATONA 기반 S/W only, look-aside, inline IPSec system 간의 성능비교를 통해 어떤 방식이 기가비트 서버 네트워크 환경에 적합한지를 검증하는 실험의 결과를 제시하였다. 전송 단의 sending speed 와 packet size 를 각각 증가시켜 IPSec 시스템의 throughput 을 측정하였고 이 측정 결과를 바탕으로 성능저하의 원인으로 예상되는 packet overhead 를 추정하였다. 본 실험은 표 1 에 제시된 조건으로 진행하였고 Finisar 사의 프로토콜 분석기인 GTX protocol analyzer[11]를 통해 성능분석을 하였다. 단 실험장비의 제약상 sending 사이드의 packet processing, encryption performance 만 평가 대상으로 삼았다. 하지만 packet processing overhead 는 양측이 동일하고 encryption 과 decryption 스피드는 비례관계이므로 실험결과의 해석에는 영향을 미치지 않을 것이라 본다.

1) Measurement of the throughput while sending speed increases: 첫 번째 실험은 패킷사이즈를 고정시키고 패킷간의 delay 조절로 전송속도를 점점 증가시켜서 throughput 변화를 측정하는 실험이다. 그림 6 의 그래프에서 볼 수 있듯이 전송속도 증가함에 따라 S/W stack 의 성능 감소가 가장 뚜렷하며 inline 방식은 감소가 거의 없었다. 이 실험을 통해 기가비트네트워크 상에서 소프트웨어 stack 의 오버헤드가 호스트 프로세서에 큰 부하를 준다는 것을 알 수 있었다. 그리고 look-aside 방식이 inline 방식보다 항상 throughput 이 낮은 이유는 look-aside 방식의 패킷오버헤드 때문일 것으로 예상된다.

2) Measurement of the throughput while packet size increases: 두 번째 실험에서는 동일한 전송속도 상에서 패킷사이즈를 증가시켜가며 대역폭 감소를 측정하였다.

표 1. 성능비교 실험조건

IPSec	system	Traffic	IPSec setting
S/W only	IPSec-tools 0.6.2[10]	UDP using packETH 1.2[9]	ESP, tunnel HMAC-SHA1, AES128
look-aside	Hifn8150[8]		
Inline	Hifn8300[8]		

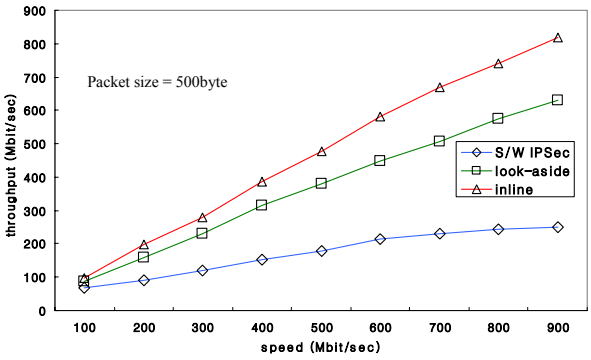

그림 6. 전송속도 증가에 따른 throughput 측정

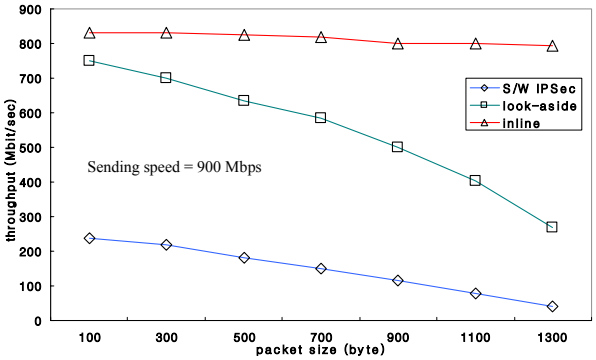

그림 7. 패킷사이즈 변화에 따른 성능 변화 측정

그림 7 에서 볼 수 있듯이 패킷의 사이즈가 증가함에 따라 look-aside 방식의 throughput 의 감소폭이 커짐을 알 수 있다. 이 역시 앞서 실험 결과와 마찬가지로 look-aside 방식의 packet processing 때문에 생기는 현상으로 보인다.

3) Approximation of the packet processing overhead: 패킷 처리시 생기는 오버헤드의 주요 원인은 버스에 관련되어 있을 거라 예상된다. III 장 그림 3 에서 알 수 있듯이 look-aside 방식에서는 크게 4 번의 버스 전송이 일어난다. 패킷의 크기가 1051 byte 이고 133Mz 의 32 비트 버스상이라고 가정하면, Packet size 가 B_{packet}, additional bus overhead 가 $C_{buspacket}$, 버스상에서 Packet 당 전송시간이 $S_{buspacket}$, 1G 네트워크 상의 packet 당 수행시간이 $S_{1Gpacket}$ 라고 할 때, 다음과 같은 추정이 가능하다.

$$B_{packet} = 1051 \text{ byte}$$

$$C_{buspacket} = (B_{packet} \times 8 \times 4) \div 32 = 1051 \text{ clock}$$

$$S_{buspacket} = \frac{C_{buspacket}}{133\ Mclock/\sec}$$

$$S_{1Gpacket} = \frac{B_{packet} \times 8\ bit}{1\ Gbit/\sec}$$

$$\therefore \quad S_{buspacket} \ : \ S_{1Gpacket} \approx 1$$

위의 추정에서 look-aside 방식의 버스 오버헤드로 인해 패킷 처리 속도가 두 배만큼 느려질 수 있음을 예상할 수 있다. 또한 S/W IPSec 은 패킷 프로세싱 외에도 cryptography 에 드는 비용이 look-aside 와 inline 시스템 보다 7~8 배정도 크다는 것이 알려져 있다[5]. 지금까지 의 실험결과를 표 2 에서 정리 요약하였다.

표 2. S/W, look-aside, inline IPSec system 성능비교

비교항목	S/W only	Look-aside	Inline	비고
Send speed 증가시	20%의 throughput	80%의 throughput	100%에 가까운 throughput	Send speed 기준
Packet size 증가시	Packet size 커질수록 throughput 급격히 감소	Packet size 커질수록 throughput 급격히 감소	100%에 가까운 throughput	Send speed 기준
Cryptography overhead	760%[5]	0%	0%	inline 기준
Packet processing overhead	최대 100%	최대 100%	0%	inline 기준

V. Conclusion

본 논문에서는 TOE 기반 look-aside, inline IPSec 시스템을 구현하고 성능 비교를 통해 기가비트 네트워크 서버 성능의 보장 가능 여부를 시험해 보았다. 이 실험을 통해 wire speed 를 보장하면서 IPSec security 를 원활히 지원할 수 있는 구조로는 inline IPSec 시스템이 아주 적합하다는 것을 알 수 있었다. 기가비트 네트워크상에서 전송속도나 패킷크기에 관계없이 좋은 성능을 보였기 때문이다. 실험결과 inline 은 소프트웨어시스템에 비해 약 8 배 look-aside 시스템에 비해 약 2 배 정도 더 좋은 성능을 가지고 있었다.

앞으로의 연구 방향은 이 결과를 IKE, storage security, VPN 같은 보다 상위레벨과 연관 지어 나가는 것이다. IKE 의 경우, 기가비트 서비스 네트워크의 단발성 패킷증가가 만든 방대한 security association 으로 야기될 IKE 의 부하 증가에 착안하여 IKE 의 내부 구조 개선을 통한 부하 해결 연구를 앞으로 진행할 수 있을 것이다.

References

[1] 권원옥, 박경, 김명준, “TCP Offload Engine(TOE) 제품동향”, 주간기술동향 2004 년 10 월 12 일.
[2] 박경, “Network I/O Acceleration Technologies”, 2005 정보과학회 컴퓨터시스템연구회 하계워크샵.
[3] R. Oppliger, *Internet and Intranet Security*, Artech House, Norwood, Mass., 1998.
[4] R. Oppliger, “Security at the internet layer,” IEEE, 1998.
[5] Robert Friend, “Making the gigabit IPsec VPN architecture secure,” IEEE Computer, vol 37, pp. 54-60, 2004.
[6] A.P. Foong et al., “TCP Performance Re-Visited,” ISPASS, 2003.
[7] O.Elkeelany, “Performance Analysis of IPsec protocol – encryption and authentication,” ICC 2002.
[8] Hifn IPSec Processors. [Online]. Available: http://www.hifn.com.
[9] packETH, [Online]. Available: http://packeth.sourceforge.net.
[10] IPSec-Tools, [Online] Available:http://ipsec-tools.sourceforge.net.
[11] Finisar GTX analyzer, [Online] Available: http://www.finisar.com.
[12] Greg Regnier et al, “TCP Onloading for Data Center Server,” IEEE Computer, Vol 37, Nov 2004.
[13] Deepak Ganesan, “Networking issues in wireless sensor networks,” July 2004, Journal of Parallel and Distributed Computing.