보안서버 성능분석 모델

윤연상, 박진섭, 한선경, *양상훈, 유영갑
충북대학교 전기전자 컴퓨터공학부
*한국전자통신연구원

Performance Analysis Model of Security Server

Yeonsang Yun, Jinsup Park, Sunkyeong Han, *Sanghoon Yang, Younggap You

School of Electrical and Computer Engineering Chungbuk National University
*Electronics and Telecommunication Research Institude
e-mail : *ysyun@hbt.chungbuk.ac.kr*

Abstract

This paper proposes a performance analysis model of security servers. Performance analysis of security server reflects both the session and data traffic load. The proposed model is the bases of estimating the maximum response time and minimum queue size of a security server comprising a session association processor whose throughput is 1000 connection/s.

I. 서론

현재 대부분의 웹 서버들이 보안을 서두르고 있다. 그 주요 원인으로 금융거래가 인터넷 시장에서 활발하게 이루어지고 있다는 것과 강력한 보안 공격이 항시 도사리고 있다는 점을 들 수 있다. 한 예로 마이크로소프트 사의 OS인 Windows 2000 server 의 경우 SSL이나 IPSEC 프로토콜 환경에서 사용 가능하도록 애플리케이션을 제공한다. OS를 통한 처리는 보안 트랜잭션 수행 시 CPU 성능의 평균 95%를 소비한다[1]. 따라서 암호화 프로세서가 내장된 전용 인터페이스 장치가 출시되고 있다[2]. 이들 장치들이 경쟁력을 얻기 위해서는 우선 보안서버에 장착했을 경우의 성능분석이 이루어져야 한다.

일반적인 서버의 데이터를 요구하거나 전달하는 목적을 갖는다. 따라서 트래픽 로드나 프로세서 역시 하나의 트랜잭션으로 모델링 된다. 이와 달리 보안서버는 IPSec/SSL 프로토콜 환경에서 사용되기 때문에 반드시 초기 핸드쉐이킹 과정을 거치게 된다. 그 후 기존의 서버환경과 유사한 트래픽 로드(데이터)를 처리하게 된다. 따라서 보안서버는 세션연결에 따른 성능분석을 수반해야 한다.

본 논문의 구성은 우선 보안서버의 성능분석에 필요한 과정을 설명한다. 그 다음 제안된 성능분석 방안으로 트래픽 로드와 모델링 방법을 소개한다. 마지막으로 보안서버의 모델링을 통한 성능분석 결과를 논한다.

II. 보안서버 성능분석 모형

본 절에서는 보안서버의 성능분석을 위해 고려해야 할 사항으로 성능 판단 기준(metric)과 트래픽 로드, 모델링 기법에 관하여 설명한다.

2.1 보안서버 성능분석 기준

일반적인 서버와 같이 보안서버의 성능은 응답시간(response time)과 처리율(throughput)로 판단할 수 있다. 응답시간은 클라이언트가 접속할 서버에게 작업을 요청한 시점부터 해당되는 작업을 완료하기까지의

시간으로 정의할 수 있다. 또한 처리율은 단위시간 동안 처리된 트랜젝션 수로 정의할 수 있다. 보안서버의 경우 세션연결을 위한 기준(metric)은 connections/sec, 데이터 처리에 관한 기준은 bytes/sec(file_transfers/sec)로 정의 된다.

2.2 트래픽 로드(traffic load)

서버 성능평가 시 고려해야 할 사항 중 우선시 되어야 할 부분이 바로 트래픽 로드(traffic load)다. 트래픽 로드는 네트워크 상태나 지역적 특성에 의해 많은 변화가 발생한다. 하지만 성능분석 대상의 서버가 어떠한 환경에서 사용될지는 알 수 있으며 이를 바탕으로 사용 환경과 가장 유사한 트래픽 로드를 발생시켜야 한다. 예를 들어 보안서버의 경우 VPN(virtual private network)내의 트래픽 로드를 고려해야 한다.

보안서버 성능분석 시 주로 사용되는 트래픽 로드는 핸드쉐이킹 과정의 트래픽 로드이다. 이 트래픽 로드를 이용하면 서버 내의 RSA 이나 Diffie-Helman 등의 프로세서 성능을 측정할 수 있다. 하지만 나머지 DES 나 MD5와 같은 암·복호화 모듈은 핸드쉐이킹 과정에서 사용되지 않으므로 성능 측정에서 제외되고 만다. 보안서버 성능 평가를 위한 트래픽 로드는 핸드쉐이킹과 데이터 암·복호화시 사용되는 보안 모듈의 성능을 모두 측정할 수 있도록 제안되어야 한다.

2.3 모델링(modeling)

실제 네트워크 장비(예를 들어, 트래픽 발생기)로 트래픽 로드를 발생시켜 서버 성능을 평가하는 과정은 비용이 많이 든다는 단점이 있다. 시뮬레이션과 같은 모델링 기술이 점차 다양화 되어감에 따라 장비 측정과 성능분석 결과가 유사하다는 결론에 이르고 있다[3]. 대표적인 모델링 기법으로 대기행렬이론(queuing theory)을 이용하는 방법이 있다[3]. 대기행렬이론은 프로세서의 성능을 측정하기 위하여 임시로 입력 큐를 설치하고 큐에 쌓이는 클라이언트의 수(패킷의 수)와 큐에서의 대기 시간을 계산하는 방법을 제시한다.

III. 트래픽 로드 제안 및 성능분석

본 절에서는 보안 프로토콜 환경에서의 세션연결 및 데이터 트래픽 로드를 제안하고 서버 모델링을 통한 보안서버의 성능분석 예를 제시한다.

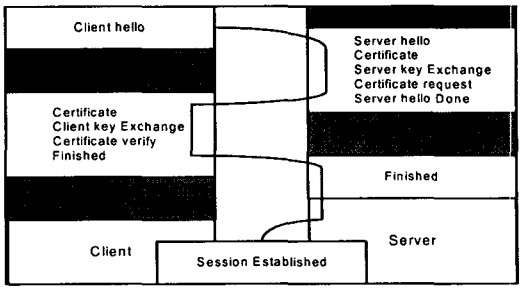
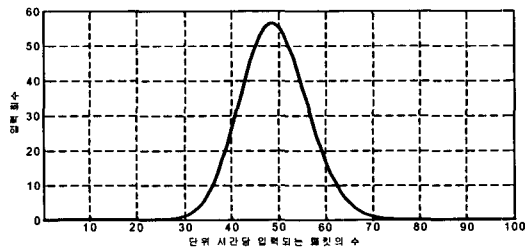


그림 1. SSL 핸드쉐이킹 과정

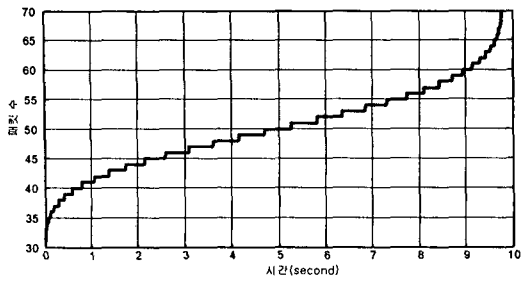
3.1 세션연결 트래픽 로드

SSL이나 IPSEC과 같은 보안 프로토콜의 경우 암·복호화에 앞서 보안 연결(security association)을 확립하는 단계가 존재한다. 이 과정의 주요 목적은 서버와 클라이언트 사이에 상호 인증(mutual certification)을 통해 서로를 확인하고 암·복호화 과정에 필요한 보안 정보를 교환함에 있다. 그림 1 에서 SSL 프로토콜의 핸드쉐이킹 과정을 나타내었다. 제안된 세션연결 트래픽은 그림 1 에서 Client_Hello 메시지에 해당된다. 서버 측면에서 보면 서버는 Client_Hello 메시지에 따라 여러 보안 메시지들을 클라이언트에게 보내게 된다. 그리고 마지막으로 Finished 메시지를 발생시킨다. 실제로 마지막의 Finished 메시지는 보안 메시지에 비해 패킷의 규모가 크지 않다[1]. 따라서 서버로 하여금 보안 메시지를 요구하는 Client_hello 가 세션연결을 위한 트래픽 로드로 정의될 수 있다.

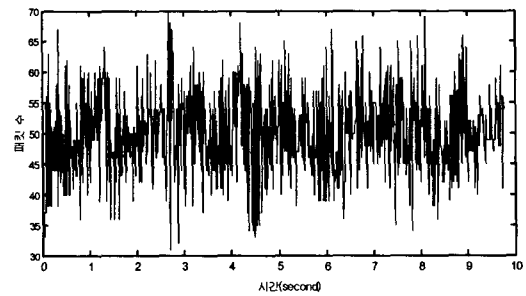
실제의 VPN과 같은 네트워크 상에서 세션연결을 위한 트래픽 로드는 프아송 분포(Poisson distribution)를 따른다. Paxon 과 Floyd의 연구에 따르면 세션연결을 위한 트래픽 로드가 시간대(hourly)에 이르면 프아송 분포를 나타낸다고 밝히고 있다[4]. 당시 네트워크 속도와 지금을 비교하면 평균 10^3 배가 증가되었다[5]. 따라서 시간대는 수 초(seconds)대로 축소될 수 있다.



(a) 프아송 확률 분포



(b) 이산 시간별 패킷 분포



(c) 연속 시간별 패킷 분포(트래픽 로드 완성)

그림 2. 세션연결 트래픽 로드

그림 2 는 제안된 세션연결 트래픽 로드의 생성 과정을 나타낸다. 프아송 확률밀도 함수를 이용하여 패킷이 입력될 확률 분포를 추출한 후[그림2-(a)] 이산 시간대 별로 패킷수를 구한다[그림2-(b)]. 마지막으로 언제 패킷이 입력될지 모르는 상황이므로 랜덤한 순서로 입력 시킨다[그림2-(c)].

3.2 데이터 암·복호화 트래픽 로드

세션연결이 끝난 클라이언트와 서버는 본격적으로 데이터를 암·복호화 하여 통신하게 된다. 세션연결 트래픽의 경우 프아송 트래픽 로드로 잘 정의되지만 데이터의 경우는 프아송 분포를 따르지 않는다[4]. 따라서 입력 분포를 실제의 네트워크 트래픽과 유사하게 모델링하는 방법 보다는 극한 상황(worst case)방식을 도입하였다. 이 방법은 실제 사용 환경에서의 성능이 측정된 성능보다 좋을 것이라는 결론을 얻을 수 있다.

그림 3 에서 worst case 방식으로 트래픽 로드을 추출한 그래프를 확인할 수 있다. 실제 입력 트래픽을 측정한 결과 단위시간당 입력되는 패킷의 최대수가 700 이었다면 이를 데이터 암·복호화시 클라이언트가 서버에게 입력하는 트래픽 로드로 정의한다.

3.3 보안서버 모델링

암호화 프로세서는 크게 세션연결과 데이터처리 트

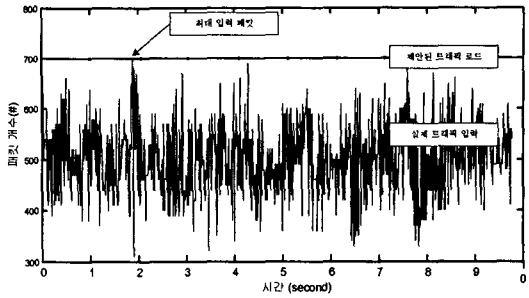


그림 3. 데이터 암·복호화 트래픽 로드(worst case)

랜젝션으로 나뉜다. 그림 4 에서 성능분석 모델을 정의하였다. 보안서버는 암호화 프로세서를 내장하였으며 서버 사용 환경으로 VPN과 같은 보안 네트워크라고 가정한다. 클라이언트는 세션연결 트래픽 로드와 데이터를 전송(또는 요청)하려는 트래픽 로드를 발생시킨다. 각각의 트래픽 로드에 대하여 보안서버는 양분된 트랜젝션(transaction)을 갖는다. 각각의 트랜젝션마다 입력 큐가 존재하고 프로세서는 처리속도(또는 처리시간)를 파라미터로 갖는다. 큐에 적제 되는 데이터 수는 프로세서의 부하를 의미하며 큐에 적제 되는 시간은 응답시간(response time)과 연관된다.

모델링을 통해 측정하고자 하는 결과는 크게 트래픽 로드 따른 세션연결 회수 또는 파일 처리량이다. 본 논문에서는 세션연결 회수를 측정하기 위하여 제안된 모델을 통한 성능분석 예를 제시한다.

그림 5 에서 제안된 세션연결 트래픽 로드에 따른 보안서버의 성능분석 결과를 나타내었다. 그림 5-(a)의 결과는 시간 경과에 따른 세션연결 회수를 나타낸다. 시뮬레이션에 앞서 세션연결에 필요한 프로세싱 과정의 처리율을 1000(connection/sec)로 설정하였다. 즉, 프로세서는 단위시간(10msec)동안 총 10회의 세션연결을 처리할 수 있으며 5-(a)에서 확인할 수 있듯이 연

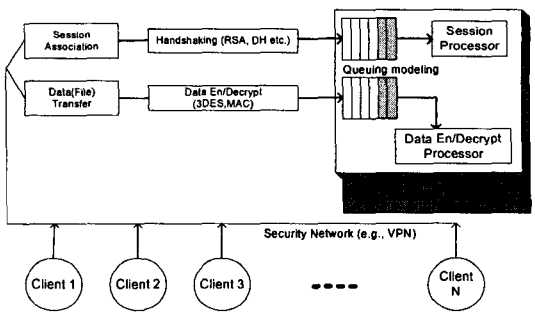
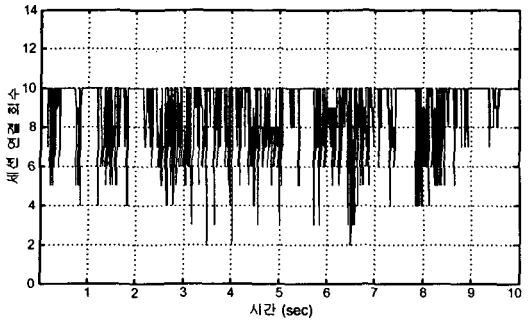
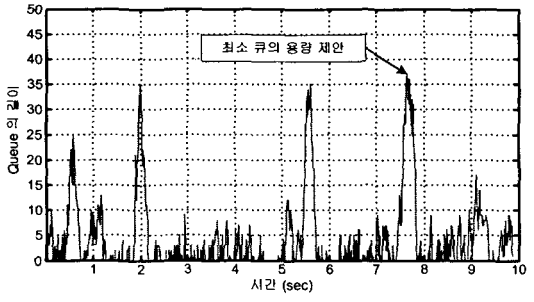


그림 4. 보안서버 성능 측정을 위한 모델링



(a)시간 경과에 따른 세션연결 회수(Throughput)



(b) 시간 경과에 따른 큐의 길이(부하)

그림 5. 큐-모델링을 통한 성능분석

결 회수가 10회에서 더 이상 증가하지 않았다. 그림 5-(b)는 입력된 트래픽 로드가 매번 처리되지 못하고 큐에서 대기하고 있는 패킷의 양을 나타낸다. 이 양을 큐의 길이라 하며 큐의 길이와 서버의 부하는 비례 관계에 있다. 또한 큐의 길이가 최고치를 나타내는 시점에서 요구되는 최소 큐의 용량을 결정할 수 있으며 클라이언트가 요청을 대기하는 최대응답시간도 고려할 수 있다. 즉, 그림 5-(b)의 최대 큐의 길이가 37이고 1회 처리시간은 1msec이므로 최대응답시간은 총 큐대기 시간과 처리시간을 합한 38msec 가 된다.

Ⅳ. 결론

본 논문에서는 보안서버의 성능평가를 위한 트래픽 로드와 서버 모델링 방안을 제안하였다. 보안서버 평가는 세션연결과 데이터 암·복호화 트래픽 로드로 구분된다. 세션연결(초기보안연결)을 위한 트래픽 로드는 프아송 입력 분포로 정의하였고, 데이터 암·복호화 트래픽은 worst case 방법을 제안하였다. 그리고 보안서버는 세션연결 프로세서와 암·복호화 프로세서로 구분하여 모델링 하였다. 본 논문에서 제시한 예로 세션연결 1000(connection/s)의 처리율을 갖는 보안서버의 경우 제안된 모델을 통해 성능을 분석한 결과 최대 응답시간은 38msec, 입력 큐의 최소 크기는 37개임을 확인하였다. 성능측정 시 입력된 세션연결 트래픽 로드는 900 request/sec 이며 이 크기는 현재 네트워크의 속도와 트래픽 양을 감안할 때 worst case에 해당된다. 따라서 위의 성능분석 결과를 보안서버의 최소사양으로 결정할 수 있다.

참고문헌

[1] "Cryptoswift secure server performance testing," www.etestinglabs.com

[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] J. Cao and M. Andersson, "Web server performance modeling using an MG1KPS queue," *10th Int'l. Conf. on Telecommunications*, vol. 2, pp. 1501-1506, Feb. 2003

[4] V. Paxson and S. Floyd, "Wide area traffic: the failure of Poisson modeling," *IEEE/ACM Transactions on Networking,* vol. 3, pp. 226-244, June 2003

[5] "인터넷 접속기술," mslab.hau.ac.kr