Anti-DDoS 로그 기록 시스템의 성능 분석

고성학*, 박능수*, 오진태**, 장종수**
*건국대학교 컴퓨터공학부
**한국전자통신연구원
e-mail:peilse@gmail.com

Performance Analysis of Anti-DDoS Logging System

Sunghak Ko*, Neungsoo Park*, Jintae Oh**, Jongsoo Jang**
*Dept. of Computer Science & Engineering, Konkuk University
**Electronics and Telecommunication Research Institute

요 약

Anti-DDoS 시스템은 분산 공격에 따라 발생하는 대량의 보안 이벤트 로그를 효과적으로 처리하여야 한다. 본 연구는 Anti-DDoS시스템에서 로그 기록에 간여 하는 모듈 간 인터페이스의 연결 및 속도 등을 분석하고 간략한 모델로 표현하였다. 이러한 모델을 기반으로 그 성능을 분석하고 시뮬레이션을 구현하였다. 구현된 시뮬레이션을 이용해 부하량 변화에 따른 로그 기록 상태를 측정하여 현재의 로그 기록 시스템의 성능을 분석하였으며, 보다 효율적인 로그 기록 시스템을 구성하기 위한 대안을 제시하고자 한다.

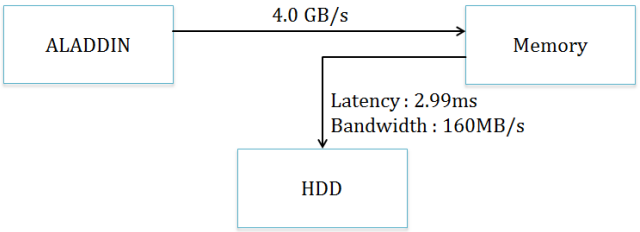
1. 서론

최근 각종 인터넷 서비스를 불가능하게 하는 DDoS(Distributed Denial of Service) 공격이 증가하고 있다. 특히 이러한 DDoS 공격은 과도한 응답을 요구함으로써 서버의 서비스를 마비시켜 사회적 경제적 피해를 발생시키고 있다. 이러한 공격을 대비하여 공격을 방어하거나 피해를 최소화하기 위한 대응방안의 연구가 진행되어 왔으며, ETRI의 Anti-DDoS시스템인 ALADDIN 역시 그 중 하나이다. Anti-DDoS시스템의 경우 DDoS공격으로 단시간에 발생하는 대량의 로그 정보를 효과적으로 기록하고 모니터링할 수 있는 기술을 필요로 한다[1].

본 논문에서는 ETRI의 Anit-DDoS시스템에서의 로그 기록 구조를 분석하여 이를 간략화 모델링으로 표현하였고, 이를 기반으로 시뮬레이션을 구축하였다. 다양한 부하 상태에서 로그 기록을 시뮬레이션을 통하여 실험함으로써, 현행 로그 기록 구조의 성능을 분석하고 향후 개선 방안을 제시하고자 한다.

2. 로그 시스템 모델링

ALADDIN 시스템은 PCI-Express 2.0 x8을 이용하여 메인 시스템과 연결되어 있으며, 로그 데이터는 PCI-Express의 버퍼에 기록되고, 일정한 양(4KB)의 데이터가 모이면 버스를 통하여 노스브리지를 거쳐 Xeon CPU내의 메모리 컨트롤러를 통과해 메모리로 기록된다. 이렇게 메모리에 기록된 로그 데이터는 일정한 양에 도달하면 또 다시 CPU, 노스브리지, 사우스브리지를 거쳐 SATA규격의 버스를 통해 HDD로 기록된다[2]. 그러나 이와 같은 시스템 전체 구조를 하나의 시뮬레이션으로 구현하기에는 구조가 복잡하고, 분석하기에도 어려움이 있다. 그러나 Bridge등 스위칭을 수행하는 노드가 Full-Duplex를 지원하고, 스위칭에서 발생하는 딜레이가 없거나 무시할 수 있을 정도로 작다고 가정하여 시스템을 단순화 할 수 있다. 특히 Anti-DDoS 시스템에서 로그 기록을 처리하는 성능을 분석하는 경우, 각 연결 스위치 간의 지원하는 최대 대역폭의 제한이 있어 이를 기반으로 각 모듈간의 인터페이스를 간략한 모델로 표현할 수 있다.



(그림 1) 간략화된 모델링

전체 시스템을 (그림 1)과 같이 데이터를 발생시키고, 저장하고, 기록하는 3개의 노드로 단순한 모델로 표현 할 수 있다. 간략화 된 모델을 시뮬레이션 하기 위하여 각 노드간의 전송 속도는 가장 속도가 낮은 버스를 기준으로 산정하였으며, 특히 HDD로의 기록 시 Seek Time을 고려하여 2.99ms의 대기 시간을 가지도록 구성되었다[3]. 시뮬레이션은 일정 Tick(1μs)을 기준으로, Tick 발생 시마다 상태 변화를 계산, 갱신하는 방법으로 구현되었다.

3. 시스템 성능 분석

본 절에서는 제안된 간략화 모델을 기반으로, 시스템의 성능을 분석을 하고자 한다. 성능 분석에 사용되는 변수는 다음과 같다: ***ER***(초당 이벤트 발생률), ***AES***(이벤트의 평

균 크기), BS_{PCI2}(PCI Express 버퍼 크기).

제안된 모델을 기반으로 주어진 시간(t) 동안에 ALADDIN에서 발생할 될 수 있는 총 이벤트 크기는 이벤트 발생률와 발생되는 이벤트의 평균 크기에 비례한다.

$$Event\,Size(t) = t \bullet ER \bullet AES \qquad (식\ 1)$$

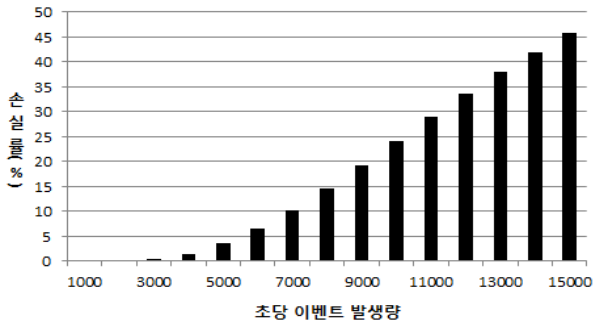
(식 1)을 이용한다면, PCI Express 2.0이 전송을 안 하고 버퍼링하는 시간을 구할 경우 그 기간 동안에 버퍼에 저장되는 이벤트의 크기를 구할 수 있다. PCI Express 2.0 브릿지의 버퍼가 채워지면 버퍼 안의 이벤트들을 메모리에 전송을 하게 된다. 따라서 PCI 버퍼에서는 버퍼링하는 시간을 가지게 되고 버퍼링 되는 시간동안에 버퍼에 저장되는 이벤트의 총 크기가 PCI 버퍼 크기보다 클 경우에는 손실이 발생한다. 따라서 이벤트 손실이 발생하는 조건은 다음과 같이 정의할 수 있다.

$$Buffering\ Time_{PCI2} \times ER \times AES \ > \ BS_{PCI2} \qquad (식\ 2)$$

4. 실험 결과 및 분석

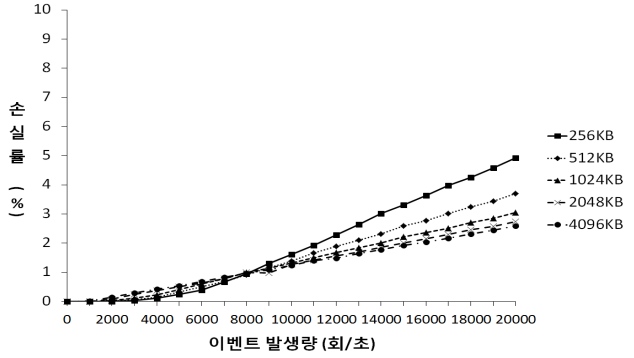
먼저 4KB의 데이터를 메모리에 축적 후 HDD에 기록할 때의 실험 결과를 정리하고 분석하였다. 실험은 실제 상황을 기반으로 다음과 같은 환경을 구성하여 진행하였다. PCI-Express Bandwidth를 4.0GB/s, Tick Time을 1000ns, 시뮬레이션 시간은 60초로 설정하였으며, 이벤트의 크기는 64, 427, 791, 1154, 1518Byte가 각각 80%, 10%, 5%, 3%, 2%의 확률로 발생하도록 설정하였다[4].

위와 같은 조건일 때, 평균 이벤트 크기(AES)는 198이다. 이에 따라 (식 1)을 응용하여 손실이 일어나는 이벤트 발생량을 구하면 6,698이 되므로, 그 이상의 이벤트가 발생할 경우 손실이 발생할 것이라 예상할 수 있다.



(그림 2) 이벤트 발생량에 따른 손실률 그래프

(그림 2)와 같이, 이벤트의 손실은 6,698에 훨씬 못 미치는 구간에서도 발생되고 있다. 6,000이하에서는 비교적 완만하게 손실률이 증가하고 있으며, 7,000이후에서부터 급격히 증가하기 시작하여 대량의 로그가 손실됨을 볼 수 있다. 6000 이하에서도 이벤트 로그의 손실이 발생하는 이유는 다음과 같이 분석된다. 본 실험에서는 임의 주기와 임의 크기로 로그 이벤트가 발생하는데, 초당 이벤트 발생량이 6000 이하에서도 큰 이벤트 여러 개가 집중이 되는 경우 일부 로그가 손실로 처리된다. 이번 실험에서는 HDD로의 Write를 요청할 때 마다 2.99ms의 Seek Time과 순수 데이터 전송 시간이 소비되므로, 요청 횟수가 많을수록 2.99ms라는 시간 소비가 더해진다. 그러므로 4KB가 아닌, 더 많은 양의 데이터를 모았다가 한 번에 쓰기를 시도하면 쓰기를 요청하는 횟수가 줄어듦으로 성능이 개선될 여지가 있다.



(그림 3) 메모리버퍼 용량에 따른 손실률 그래프(256~4096KB)

메모리버퍼의 용량을 점차 늘려가면서 실험을 진행하였다. (그림 3)에서 보는 바와 같이, 용량을 늘리면 늘릴수록 손실률이 낮아지는 모습을 확인할 수 있다. 그러나 높은 용량대로 갈수록 그 효과가 크게 나타나지 않는다. 게다가 256KB이상의 용량에서는 8,000회 이하의 비교적 낮은 이벤트 발생량일 때에 오히려 손실률이 높아지는 경우를 확인해 볼 수 있다.

5. 결론

본 논문에서는 로그 기록 시스템에서 로그 손실을 초래하는 원인을 실험적으로 분석하였으며, 이 결과 로그 손실의 주요 원인이 저장 장치의 지연시간임을 증명하였다. 또한 실험 결과를 통해 안정적인 로그 기록 환경 구성을 제안하였다. 이를 통해 더욱 안정적인 로그 기록 환경을 설계하기 위한 기초 자료로서 활용할 수 있다.

향후 현재 검증한 메모리 버퍼 크기를 통한 개선 방안 외에, 보다 효율적인 개선 방안에 대한 연구가 필요하다.

참고문헌

[1] 천준호, 신동규, 장근원, 전문석 “DDoS공격에 대한 방화벽 로그 기록 취약점 분석” 정보보호학회 논문지 제17권 제6호 Dec 2007

[2] “S5520HC Server Mainboard data sheet” Intel Inc.

[3] “Seagate savvio 10K RPM Hard Disk Drive Data sheet” Seagate Inc.

[4] James F. Kurose, Keith W. R “Computer Networking” 5Th Ed. Addison-Wesley