안전한 네트워크를 위한 보호조치 대응 시점

이재성*, 지정은*, 임휘빈*, 신용태*
*숭실대학교 컴퓨터학과
e-mail:jslee@cherry.ssu.ac.kr

Measurement of Management Point for Secure Network

Jae-Sung Lee*, Jung-Eun Ji*, Hui-Bin Lim*, Yong-Tae Shin*
*Dept of Computing, Soong-sil University

요 약

최근 네트워크의 가용성을 침해하는 DDoS공격으로 국내외 주요 사이트가 마비되는 사건이 있었다. 본 논문에서는 TCP와 UDP의 자기유사성을 이용하여 유효 대역폭을 측정하고 네트워크의 가용성을 보장하기 위한 한계 대응 시점을 예측하였다. 그리고 실험을 통해 한계 대응 시점의 예측이 정확함을 확인 할 수 있었다.

1. 서론

최근 7.7 DDoS 대란이 발생하여 국가기관 및 주요 기업의 사이트가 마비되었다. 당시 좀비 PC의 공격 기법으로 주로 Flooding 공격이 사용되었다. Flooding 공격은 네트워크의 대역폭 및 보안장비의 부하를 유발하여 최종적으로 네트워크의 가용성을 떨어뜨려 정상적인 서비스를 제공하지 못하게 하는 공격방법이다. 가용성을 목표로 하는 공격은 대응 시점을 파악하고 초기에 대응하는 것이 가장 좋은 대처 방안이 될 것이다.

본 논문에서는 보안 목표 중 네트워크 가용성을 보장하기 위한 한계 대응 시점을 연구하였다. 연구 방법으로는 자기유사성을 갖는 트래픽에 대한 유효 대역폭을 계산하고, 네트워크 또는 시스템의 대역폭을 측정한 임계치를 기준으로 한계 대응 시점을 예측한다.

본 논문의 2장에서는 관련 연구로 트래픽의 자기유사성 및 유효 대역폭과 네트워크 대역폭 측정 방법에 대하여 알아보고, 3장에서는 한계 대응 시점을 구하는 방법과 실험을 통하여 한계 대응 시점을 예측한다. 4장에서는 결론을 논할 것이다.

2. 관련연구

2.1 트래픽의 자기유사성과 유효 대역폭

트래픽의 자기유사성은 트래픽이 시간 규모에 관계없이 군집성을 가지는 특성이다. W. E. Leland의 연구에서 트래픽이 자기유사성을 가진다는 사실을 증명된 이후 인터넷 트래픽이 자기유사성을 가지는 것을 밝히려는 연구가 진행되었다. 그 결과 TCP, UDP 트래픽이 자기유사성을 가짐이 증명되었다[1]. DDoS Flooding 공격은 주로 TCP와 UDP를 이용한다[4]. 따라서 본 논문에서의 모든 트래픽을 TCP, UDP 그리고 그 외의 트래픽으로 분류한다.

Norros[2]는 자기유사성을 가지는 트래픽의 유효 대역폭을 측정하였다. 유효 대역폭은 트래픽 흐름을 위해 네트워크가 할당해야 하는 대역폭을 의미한다. 해석적 모델로서 유효 대역폭을 측정하는 공식은 다음과 같다.

$$C = m + (\kappa(H)\sqrt{-2\ln\epsilon})^{1/H} a^{1/(2H)} x^{-(1-H)/H} m^{1/(2H)}. \qquad \text{식(1)}$$

식(1)에서 a는 트래픽 스트림의 분산계수이고, x는 버퍼의 크기이다. m은 트래픽 스트림의 평균 비트율이며, H는 허스트 파라미터이다. 마지막으로 ϵ는 목표로 하는 셀 손실률이다. 이 공식에서 중요한 값은 a와 H이며, 이 요소는 결과 값에 큰 영향을 준다.

2.2 네트워크 대역폭 측정[3]

네트워크 사용 가능성을 알아보기 위한 네트워크 대역폭 측정 방법에는 크게 두 가지가 있다. 패킷이나 패킷 트레인을 네트워크에 전송하여 계산하는 방법과 시스템의 하드웨어 자원으로 대역폭(처리율)을 측정하는 방법이다. Jin의 시스템 I/O 처리율 공식은 식(2)와 같다.

$$IOthroughput = \frac{MemoryBandwidth}{\frac{MemoryClock}{IOBus\,Clock} + 2} \qquad \text{식(2)}$$

3. 제안

본 절에서는 네트워크의 가용성을 보장하기 위해 트래픽을 분석하여 한계 대응 시점을 예측 하고자 한다.

3.1 실험 환경

한계 대응 시점을 구하기 위해 서버 한 대와 클라이언

트 PC 한 대 그리고 1000 Base T의 연결 링크로 소규모 네트워크를 구성하였다. 서버에는 VIA 868 PCI 컨트롤러가 있는 ASUS K7V 메인보드를 장착하였다. VIA 868 PCI 컨트롤러는 133MHz 메모리 버스와 144MB/s 메모리 복사 대역폭을 가지고 있다. 메모리는 SDRAM 512MB이며, 네트워크 카드는 Realtek 8029 PCI NIC, 운영체제는 Windows 2000 Professional을 사용했다.

3.2 한계 대응 시점 예측 방법

서버에서 수신하는 트래픽을 분석하여 시스템의 가용성을 보장하기 위해 늦어도 대응해야 하는 한계 대응 시점을 구하는 방법은 다음과 같다.

1. 서버는 링크 상에 수신되는 트래픽(TCP, UDP, 그 외 트래픽)을 분류하고 트래픽의 양을 측정한다.
2. 식(2)을 이용하여 자기유사성을 갖는 TCP, UDP의 유효 대역폭을 계산한다. 이 때, TCP의 허스트 값은 0.93, UDP의 허스트 값은 0.90로 한다[4].
3. TCP, UDP의 유효 대역폭과 그 외의 트래픽 Rt를 합산하여 총 유효 대역폭인 C_{total}을 구한다.
4. 유효 대역폭의 변화율, $VariationRate$을 계산한다.
5. 수신된 트래픽이 임계치까지 이르는 시간 t를 구하는 전체 공식은 다음과 같다.

$$[t] \le (\log_{VariationRate} \frac{critical\,value}{C_{total}}) - 1 \qquad \text{식(3)}$$

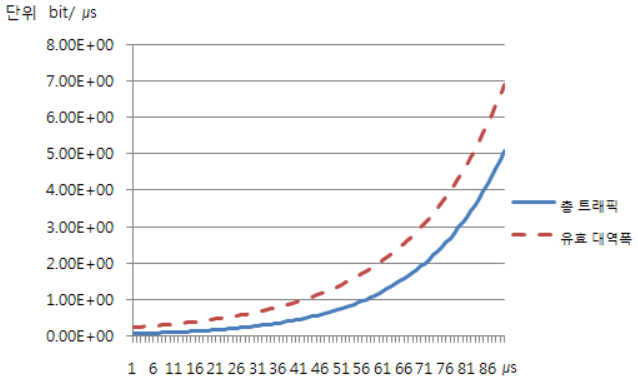
식(3)에서 $critical\,value$는 임계치로 네트워크와 시스템의 최대 처리율을 의미한다. 임계치를 선정하는 방법은 네트워크의 링크 대역폭이 시스템의 처리율보다 클 경우 링크 대역폭이 임계치가 되며, 반대의 경우에는 시스템의 처리율이 임계치가 된다. C_{tcp}와 C_{udp}는 각각 TCP와 UDP의 유효 대역폭이며, Rt는 TCP, UDP 이외의 모든 트래픽양이다. $VariationRate$는 유효 대역폭의 변화율이다.

3.3 한계 대응 시점을 예측하기 위한 실험

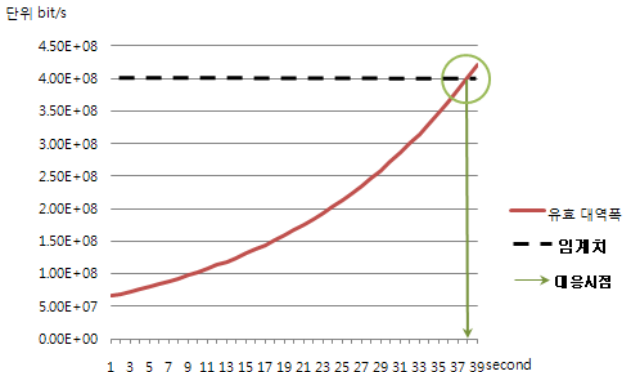
총 유효 대역폭과 유효 대역폭 변화율을 구하여 제안한 한계 대응 시점을 예측하기 위한 실험을 하였다. 유효 대역폭 측정을 위한 파라미터 값으로 a는 1.7107, x는 10^8, ϵ는 10^{-6}으로 설정하였다. 클라이언트에서 서버로 전송되는 초기 트래픽으로 TCP, UDP, Rt는 각각 50 Mbps, 10 Mbps, 3 Mbps으로 총 63 Mbps을 전송하였고, 매 초마다 5%를 증가시켰다.

실험 결과, 식(2)을 통하여 최적의 임계치 384Mbps를 구하였다. (그림 1)에서는 트래픽이 증가에 비례하여 유효 대역폭이 증가함을 볼 수 있었고, (그림 2)에서는 예측한 한계 대응 시점 t = 38이 실제 결과 값과 일치함을 알 수 있었다.

따라서, 자기유사성을 지닌 트래픽을 분석 하고 한계 대역폭을 계산하여 한계 대응 시점을 예측할 수 있었다.



(그림 1) 트래픽과 유효 대역폭



(그림 2) 유효 대역폭으로 예측한 한계 대응 시점

4. 결론

본 논문에서는 자기유사성을 가진 트래픽의 유효 대역폭을 측정하여, 한계 대응 시점을 예측하였다. 하지만 실험 환경이 소규모 네트워크이고, 적은 트래픽 양으로 측정하였기 때문에 트래픽과 유효 대역폭의 차이가 미비하게 측정되었다. 그러나 실제 Gbyte 단위의 네트워크에서는 분명한 차이를 보일 것으로 예상된다.

향후, 제안된 방식을 토대로 대규모 네트워크에서 가용성을 보장하기 위한 한계 대응 시점에 관한 연구가 필요하다.

참고문헌

[1] 박정숙, 전용희 "자기유사 트래픽 특성을 고려한 차등서비스 망의 성능평가" 한국통신학회논문지, Vol.33 No.5, 2008.05

[2] I. Norros "On the use of fractional Brownian motion in the theory of connectionless networks" IEEE Journal on Selected Areas in Communication, Vol.13, No.6, pp.53-962, 1995

[3] G. Jin, B. Tierney "System Capability Effects on Algorithms for Network Bandwidth Measurement" Proceedings of the. Internet Measurement Conference , 2003.10

[4] 홍승범, 박재성, 황주영, 이재용 "다중화된 IP 트래픽의 자기유사성에 관한 연구" 2000년 추계종합학술발표회 논문집, pp.519-522, 2000.11