연결설정 지연 단축을 위한 적응적 비율 제한기의 설계 및 구현

*심재홍
*조선대학교
*jhshim@chosun.ac.kr

Design and Implementation of Adaptive Rate Limiter for Reducing Connection Delay

*Jaehong Shim
*Chosun Univ.

요 약

새로운 연결요청(connection request) 패킷의 전송비율을 일정 비율 이하로 제한함으로써 웜을 탐지하는 바이러스 쓰로틀링(virus throttling)[3]은 대표적인 웜 조기 탐지 기술 중의 하나이다. 기존 바이러스 쓰로틀링은 비율 제한기의 주기를 고정시키고 지연 큐 길이만으로 웜 발생 여부를 판단한다. 본 논문에서는 가중치 평균 지연 큐 길이를 적용하여 비율 제한기의 주기를 적응적으로 조절하는 알고리즘을 제안하고, 가중치 평균 지연 큐 길이에 따른 다양한 주기결정 기법을 제시한다. 실험결과 제안 알고리즘은 웜 탐지시간에는 크게 영향을 미치지 않으면서도 연결설정 지연시간을 단축하여 사용자가 느끼는 불편함을 줄여 줄 수 있음을 확인하였으며, 또한 복잡한 주기결정 방법보다는 현재의 가중치 평균 큐 길이에 비례 또는 반비례하는 방식으로 비율 제한기의 주기를 결정하는 것이 가장 효과적이라는 것을 실험을 통해 확인하였다.

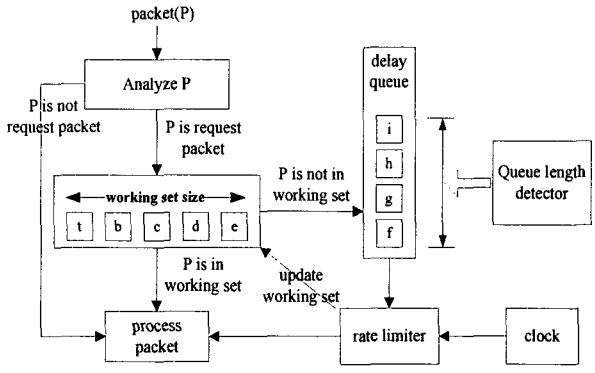
I. 서 론

인터넷을 기반으로 하는 많은 웜(worm)[1,2]들은 스스로 전파되는 속성을 가지며, 주로 인터넷상에 존재하는 호스트의 응용 프로그램들의 취약성을 이용한다. 따라서 웜에 감염된 호스트는 취약성이 있는 또 다른 호스트를 찾기 위해서 대상 호스트의 IP 주소를 무작위로 생성하여 스캐닝을 하고, 스캐닝한 정보를 이용하여 다른 호스트에 웜 코드를 전파한다.

이처럼 스스로 전파되는 웜이 유해한 데이터를 전달하지 않을지라도 웜의 전파과정에서 발생하는 엄청난 양의 트래픽은 네트워크의 성능을 저하시킬 뿐 아니라, DDOS 공격 등도 가능하게 한다. 또한 웜의 전파 속도가 워낙 빠르기 때문에 사용자들이 일일이 그것에 대항하여 반응하기에는 역부족이다. 따라서 새로운 웜이 발생하였을 때 웜의 발생 여부를 빠르게 탐지하여 더 이상의 웜 전파를 차단해야 한다.

그러나 정상적인 트래픽은 상당히 낮은 비율(초당 약 1개)로 연결요청이 이루어지며, 또한 연결 대상시스템이 웜처럼 불특정 다수가 아닌 소수의 특정 시스템들로 국한되어 있다. 따라서 웜과 정상 트랙픽의 이 같은 속성 차이를 이용하면 쉽게 웜 발생을 탐지할 수 있다.

바이러스 쓰로틀링[3]은 새로운 세션의 연결(connection) 비율을 제한하여 웜의 전파 속도를 늦추고 차단하는 기법이다. (그림 1)은 바이러스 쓰로틀링 기법에 의해 제어되는 전송 패킷들의 흐름을 나타낸 것이다. 새로운 연결요청 패킷(P)의 전송요청이 들어오면 워킹 셋(working set)에서 P와 동일한 수신 IP 주소가 존재하는지 확인하고, 만약 존재한다면 P를 정상 트래픽으로 간주하여 지연 없이 즉시 전송한다. 그렇지 않은 경우 P를 지연 큐(delay queue)에 저장한다. 즉, 상대적으로 최근에 접속이 이루어졌던 호스트에 대해서는 지연 없이 바로 연결요청 패킷을 전송하고 그렇지 않은 호스트에 대해서는 패킷을 지연 큐에 보관한 후 적당한 시기에 비율 제한기(rate limiter)에 의해 전송되게 한다. 비율 제한기는 일정 시간 간격을 두고 주기적으로 지연 큐에서 제일 오래된 패킷을 꺼내어 이를 전송한다. 이때 이 패킷과 동일한 수신 IP 주소를 가지는 지연 큐 내의 다른 패킷들도 동시에 전송한다. 비율 제한기는 매 패킷을 처리할 때마다 해당 패킷의 수신 IP 주소를 워킹 셋에 추가한다. 마지막으로 지연 큐 길이 감시자(queue length detector)는 패킷이 지연 큐에 저장될 때마다 지연 큐의 길이를 검사하여 사전에 정의된 경계값(threshold: 일반적으로 큐 크기임)을 초과하면, 웜이 발생하였다고 판단한다. 일단 웜이 탐지되면 시스템은 모든 패킷을 차단하여 더 이상의 웜 전파를 차단한다.



(그림 1) 바이러스 쓰로틀링(virus throttling)

기존의 바이러스 쓰로틀링에서는 비율 제한기의 주기를 1초로 고정시켰다. 이 경우 일시적으로 새로운 세션에 대한 연결 요청이 폭주할 경우 지연 큐에 늦게 삽입된 연결요청 패킷들은 상당한 지연시간을 가지게 되며,