적응적 비율 제한기의 주기 결정을 위한 파라미터 선택

*심재홍, +김판구
조선대학교 컴퓨터공학부
*jhshim@chosun.ac.kr, +pkkim@chosun.ac.kr

Parameter Selection for Determining Period of Adaptive Rate Limiter

*Jaehong Shim, +Pankoo Kim
Chosun Univ., Dept. of Computer Engineering

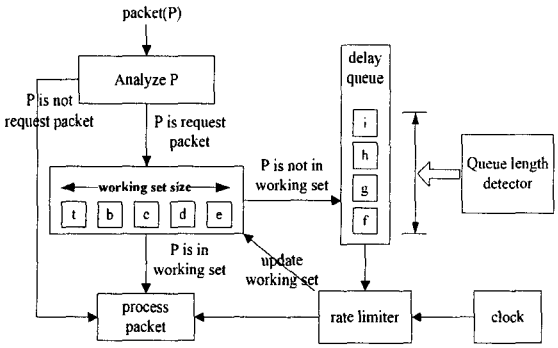
요 약

바이러스 쓰로틀링(virus throttling)은 새로운 연결요청(connection request) 패킷의 전송비율을 일정 비율 이하로 제한함으로써 웜을 탐지하는 대표적인 웜 조기 탐지 기술 중의 하나이다. 기존 바이러스 쓰로틀링 연구에서는 웜 탐지시간에는 크게 영향을 미치지 않으면서도 연결설정 지연시간을 단축시키기 위해 가중치 평균 지연 큐 길이를 적용하여 비율 제한기의 주기를 적응적으로 조절하였다. 그러나 기존 연구에서는 비율 제한기의 최소주기를 고정하고 또한 주기 값을 감소시키다가 다시 증가시키기 시작하는 반환점도 미리 고정하였다. 그러나 이러한 두 파라미터는 설정된 값이 무엇인가에 따라 웜 탐지시간과 연결설정 지연에 서로 다른 영향을 미친다.

본 논문에서는 적응적 비율 제한기의 두 파라미터인 최소주기와 반환점이 웜 탐지시간과 연결설정 지연에 미치는 영향을 실험을 통해 분석하고, 상황에 따라 적절한 파라미터 값을 설정할 수 있는 방안을 제시하고자 한다. 제안된 방법은 파라미터를 고정시킨 기존방법보다는 웜 탐지시간이나 연결설정 지연시간 단축에 더 효율적이라는 사실을 실험을 통해 확인하였다.

I. 서 론

바이러스 쓰로틀링[1,2]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.



(그림 1) 바이러스 쓰로틀링(virus throttling)

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 가장 오래된 패킷을 꺼내어 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 탐지 되면 시스템은 패킷 전송을 중단하여 더 이상의 웜 전파를 차단한다.

본 연구팀은 비율 제한기의 주기를 고정시키고 지연 큐 길이만으로 웜 발생 여부를 판단하는 기존 바이러스 쓰로틀링의 방법을 탈피하고, 가중치 평균 지연 큐 길이를 적용하여 비율 제한기의 주기를 적응적으로 조절하는 적응적 비율 제한기를 제안하였다[3]. 기존의 제안된 적응적 비율 제한기의 기본 아이디어는 다음과 같다.

평균 지연 큐 길이가 증가하기 시작할 경우 웜 때문인지 아니면 일반 패킷의 일시적 증가인지 구분하기 힘들기 때문에 기존 바이러스 쓰로틀링과 같이 비율 제한기의 주기를 고정시켜 운영한다. 이때 큐 길이가 꾸준히 계속 증가하면 웜일 가능성이 크고, 증가하다가 감소하기 시작하면 일시적인 트래픽 증가일 가능성이 높다. 평균 큐 길이가 감소하기 시작하여 일시적인 트래픽 증가로 판단될 경우 비율 제한기의 주기를 서서히 감소시켜 점점 빠르게 지연 큐 내에 대기 중이던 연결요청 패킷을 외부로 전송한다. 그래도 계속해서 평균 큐 길이가 감소하여 큐 길이가 짧아지면 이번에는 반대로 주기를 다시 증가시켜 서서히 원래의 주기로 되돌아 오게 하는 것이다. 만약 평균 큐 길이가 다시 증가하기 시작하면 웜 탐지시간에 영향을 미치지 않게 비율 제한기의 주기를 원래 주기로 바로 복원한다. 이러한 전략은 기존의 웜 탐지