서비스 거부 공격에 대응한 웹서버 가용성 향상을 위한 운용 정책 방안

정회원 백 남 균*, 종신회원 정 수 환*°

Operation Policy for Enhancing Availability of a Web Server against DoS Attacks

Namkyun Baik* *Regular Member*, Souhwan Jung*° *Lifelong Member*

요 약

본 연구에서는 네트워크 기반 서비스거부공격에 대응하여 웹서버의 가용성을 향상 시킬 수 있는 보안노드를 설계하고자, 과부하 상태에서 문서의 인기도에 기반 하여 신규 세션 허용을 제어할 수 있는 동적 서비스 메커니즘을 품질 향상방안으로 제안하였다. 그 결과, 과부하가 지속될수록 기존 방식에 비해 웹서비스 요청 세션에 대한 연결접속률과 연결완성률이 크게 향상됨을 알 수 있었다.

Key Words : DoS, 웹서버, 가용성, Zipf's Law

ABSTRACT

This paper proposes a 'secure node' to be robust against network-based DoS attacks. The secure node selectively accepts new sessions based on the Zipf's law while a link is in the overload state. Our scheme calculates a threshold value for overload state, and provides a dynamic service mechanism for enhancing availability of a web server. The simulation results show performance improvement of the proposed scheme in terms of completion/connection ratios.

I. 서 론

인터넷 보급에 따른 정보 교환 및 공유 확대로 인하여, 인터넷은 다양한 정보시스템에 활용되어 기본 인프라로 정착될 것이며 그 가치와 응용은 더욱 높아질 것이다. 이렇게 정보화가 진전되는 반면에 이에 대한 역기능도 점차 심화되고 있으며 다양한 침해유형 중 네트워크 기반 서비스 거부 공격은 정보보안과 침해영향력에 있어 가장 위협적인 존재이다. 여러 보고서에 따르면 서비스거부공격 대상이 되는 국가 중 우리나라가 아시아권에서 중국에 이어 2번째로 높은 것으로 나타났으며 과거에는 국내 웹서버들이 공격의 경유지로서만 악용되는 경우가 많았지만, 이제는 직접적인 공격의 대상으로 이러한 경향은 앞으로 더욱 증가할 것으로 보인다[1][2].

특히, 웹서버는 불특정 다수를 대상으로 서비스를 제공하므로 침입차단을 위한 접근제어방식으로 보안정책을 수립할 수 없어 보안수준 강화에 어려움이 있다. 이에 대응하기 위해 우선적으로 공격에 감내할 수 있는 네트워크 대역폭과 서비스 노드 용량 확보를 통한 물리적 대응이 고려될 수 있으나 적정수준의 비용대비 효과를 고려하면 그와 같은

※ 본 연구는 숭실대학교 교내연구비 지원에 의해 수행되었습니다.
* 숭실대학교 정보통신전자공학부 통신망보안 연구실 (namkyun@kisa.or.kr, souhwanj@ssu.ac.kr) (° : 교신저자)
논문번호 : KICS2008-03-122, 접수일자 : 2008년 3월 10일, 최종논문접수일자 : 2008년 7월 23일

환경 구축은 현실적으로 불가능하다. 이외 제안된 방어기술로 null0 라우팅, uRPF 등의 기술이 있으나 이 역시 적용과 구현의 한계로 인하여 현실적인 과부하 공격 대응책으로는 부적절하다[3][4][5].

이에 본 연구에서는 웹서버에 대한 서비스거부공격에 대응하여 가용성을 유지할 수 있는 보안노드를 설계하고자, 웹 트래픽에 대한 특성을 반영하여 과부하 상태에서 문서의 인기도에 기반 하여 서비스를 제공하는 동적 메커니즘을 가용성 향상방안으로 제안하고 이에 대한 성능향상을 분석하고자 한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 웹서버의 서비스거부공격에 대응하여 기존에 연구되었던 대응 기법들을 설명한다. Ⅲ장에서 웹 트래픽 특성을 활용한 웹서버 가용성 향상을 위한 동적 메커니즘을 제안하며 Ⅳ장 실험 및 검토에서는 시뮬레이션을 통해 제안된 방법의 효율성을 비교·분석하고 Ⅴ장에서 마지막으로 결론을 정리한다.

Ⅱ. 기존의 연구 동향

인터넷 프로토콜(IP)이 큰 성공을 거둔 이유 중의 하나는 단순성에 있다. IP의 기본 디자인 원리는 네트워크 종단인 출발지와 목적지 노드에 많은 기능을 부여하도록 하고, 네트워크 전역에 걸쳐 있는 중간 노드들은 단지 포워딩 기능만을 수행하면 된다. 즉, 모든 트래픽을 동일한 중요도를 가진 최선형(best-effort) 방식으로 처리하기 때문에 갑작스런 트래픽 폭주(busty)로 인하여 경로에 혼잡이 발생할 경우 원하는 트래픽만을 선별하여 서비스를 제공할 수 없다[6][7]. 즉, 종단 네트워크 또는 시스템 자원 한계 초과로 서비스에 대한 가용성 침해가 발생하며 해당 서비스가 거부되어 진다. 이는 웹서버에도 동일하게 적용되며 대표적인 공격유형으로 그림 1과 같이 syn flooding과 같은 시스템 기반과 DDoS(Distributied Denial of Service)와 같은 네트워크 기반 서비스거부공격이 있으며 과부하 공격 부하량에 반비례하여 웹서버의 서비스 확률은 줄어든다.

이러한 서비스거부공격이 증가함에 따라 각 ISP에서도 각종 네트워크 장비나 보안솔루션을 동원하여 네트워크 모니터링과 유해 트래픽 차단 등의 조치를 취하고 있지만 광대역 네트워크 환경 하에서는 아직 만족할 만한 대응을 수행하고 있는 수준은 아니다.

본 장에서는 지금까지 서비스거부공격에 대해 어떠한 방법으로 대응을 하고 있었는지 살펴보고 그 방법들의 한계점을 살펴보기로 한다.

가장 일반적인 유해 트래픽 차단 기술로 접근통제목록(Access Control List)을 이용한 필터링 기능이 많이 활용되나 이 기능만으로는 공격을 방어하기는 어렵다. 라우터를 예를 들면, Ping 공격 같은 인터넷 통신에 꼭 필요하지 않은 몇 가지 간단한

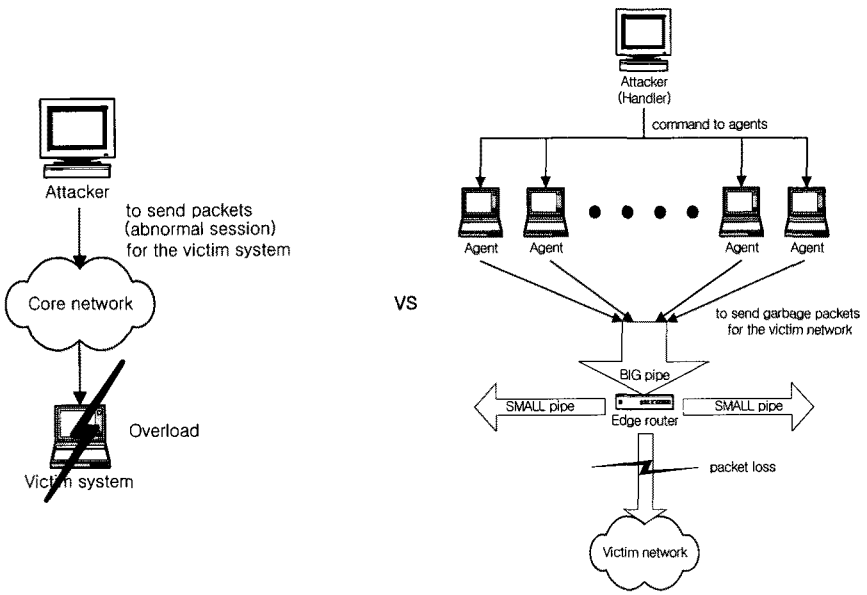


그림 1. 시스템 기반 및 네트워크 기반 서비스 공격

공격에 대해서는 필터링 메커니즘을 통해 방어할 수 있다. 하지만 웹서버 공격은 HTTP라는 필수적인 프로토콜을 사용하기 때문에 특정 프로토콜 자체를 모두 필터링하는 방법은 사용할 수가 없는 것이다. 또한, 접근통제목록 기능은 출발지 주소가 위장 되었는가 여부에 상관없이 HTTP 에러와 HTTP half-open 커넥션 공격 같은 애플리케이션 레이어의 공격에 대해선 그 효과를 발휘하기 어렵다는 한계점을 가진다[3].

Null0 Routing은 특정한 목적지(Victim)로 향하는 패킷들을 Null0 라는 가상 인터페이스인 일종의 폐기 장소로 보내서 소멸시키는 기술이다. 이 기술은 국외에서는 블랙홀 라우팅 또는 블랙홀 필터링이라고 불리고 있지만, 국내에서는 대부분 Null0 라우팅이라고 한다. 이 기술은 네트워크 장비의 기본 기능인 포워딩 기능을 이용하므로 ACL 기술에 비해 장비의 과부하가 거의 없으나, IP 기반(L3)의 필터링만 제공할 수 있고, 서비스 포트(L4)나 컨텐츠(L7)에 의한 필터링은 불가능한 단점을 가지기에 웹서버에서는 활용할 수 없다. 또한 해당 목적지로 전송되는 악성공격 패킷들뿐만 아니라 정상적인 패킷들도 포함한 모든 트래픽이 소멸되기 때문에 이 방법은 원천적인 해결책이 될 수가 없다[4].

uRPF(unicast Reverse Path Forwarding) 기법은 출발지 IP 주소를 위장한 공격을 차단해 줄 수 있는 기술로써, 라우터가 패킷을 받으면 출발지 IP 주소를 확인하여 해당 IP로 갈 수 있는 역경로(Reverse Path)가 존재하는지 확인함으로써 출발지 IP 주소의 신뢰한다. 대부분의 서비스거부공격이 자신의 출발지 주소를 위장하므로 uRPF는 상당히 효과적인 서비스거부공격 차단 수단이 될 수 있다. 하지만, 이 기술 역시 다수의 라우팅 경로가 존재하는 비대칭 망구조를 가지고 있을 경우 적용과 구현의 한계가 있으며 위장 주소 패킷 전송을 방지하는 것 이외에 과부하를 이용한 웹서버 서비스거부공격에 대한 대응 기능으로는 적절하지 않다[5].

Rate-Limit 방식은 특정 서비스 또는 패턴을 가진 패킷이 단위시간 동안 일정량 이상 초과할 경우 그 이상의 패킷을 통과시키지 않도록 하는 기법이다. rate filtering이라고도 하며, Cisco에서는 CAR(Commit Access Rate)로 구현하고 있다. 또한, 이 기법은 Syn flooding 공격 시 Syn 패킷의 Bandwidth 제한, Smurf 공격 시 ICMP 패킷의 Bandwidth 제한 등에 유용하게 사용될 수 있다. 하지만, 비정상적인 패킷 뿐만 아니라 정상적인 패킷도 무분별하게 차단될 수 있다[8].

Traffic Shapping은 네트워크를 통신 폭주 상태로 만들 수 있는 통신량 급증을 제한하기 위해, 데이터는 대기열 버퍼로 처리된 다음, 조절된 크기로 네트워크로 보내지면 부하분산 효과로 약속된 트래픽 부하를 유지할 수 있다. 하지만, 수분이상 지속되는 과부하에 대해서는 대기열 버퍼와 처리용량 제한이 있어 그 효과가 미비하며 Rate-Limit 방식과 동일하게 비정상적인 패킷 뿐만 아니라 정상적인 패킷도 무분별하게 차단될 수 있는 단점이 있다.

마지막으로 로드 밸런싱 혹은 이중화, 삼중화 등을 통해서 더욱 용량이 큰 트래픽에 대해서도 처리할 수 있도록 네트워크의 대역폭 및 성능을 강화시키는 방법이 있다. 하지만, 이런 방법은 비용 대비 효과적인 대안이 되지 못한다고 할 수 있다. 또한 비용 대비 효과 문제를 떠나서라도, 결국 얼마간 기간이 지나면 또다시 그 용량을 초과하는 형태의 공격이 발생하게 될 것이 자명한 일이기 때문에 임시방편에 그칠 수 있는 것이다.

Ⅲ. 웹서버 가용성 향상을 위한 동적 메커니즘

3.1 웹트래픽 특성

웹트래픽 특성을 분석하기 위해서는 웹서비스를 제공하기 위해 사용되는 HTTP 프로토콜 이해가 필요하다. HTTP는 요청-응답 동작을 기본으로 송수신되는 문서의 위치는 URL로 지정된다. 초기 버전인 HTTP/1.0은 연결설정 후 클라이언트가 요청 메시지에 응답메시지 송신 완료 후 연결을 종료하는 상태없는(stateless) 프로토콜로 각 문서 당 세션 연결을 수립하고 해지하므로 한번 접속에 여러 세션이 필요하다. 그러나 상태 없는 연결은 자원을 요청할 때마다 각각의 TCP 연결을 새로 설정해야만 하는 번거로움이 있고 연결 설정 때문에 시간 또한 오래 걸린다. 이러한 단점 때문에 HTTP/1.1에서는 지속적인(persistent) 연결 유지를 수행하도록 '파이프라인' 개념을 도입하였다. 즉, 전송을 위한 요청 및 응답 마다 새로운 세션을 수립하는 것이 아니라 하나의 세션 연결을 통해 여러 요청 또는 응답을 보낼 수 있도록 수정하여 이전 하위 버전에 비해 접속 세션수를 감소시켜, 전송 속도의 향상과 연결 설정에 따른 부하를 줄였다[9][10]. 하지만, 여전히 1개 이상의 다수 개 세션은 반드시 존재하게 되며 필요로 하는 세션의 연결과 완성 정도가 서비스 품질의 바로미터로 활용될 수 있으며 뒷장에서 이에 대해

추가 설명한다.

웹트래픽 특성 즉, 인터넷 트래픽 특성에 대해서 여러 방면의 연구가 활발히 진행되고 있으나 지금까지도 트래픽의 통계적인 특성이 포아송(poisson) 특성을 따르는지 아니면 자기유사(self-similarity)한 특성을 보이는지에 대해서는 많은 논란이 되고 있다. 본 논문에서는 어느 한쪽의 논리를 일방적으로 수용하기 보다는 전송 및 응용수준으로 나누어 각각에 대해 서로 다른 특성 모델을 가정하여 수용함으로써, 서로간의 보완을 유도할 수 있는 적절한 통제 기법에 활용될 수 있도록 한다[11][12].

3.1.1 전송계층 기반 특성

OSI의 중간 계층인 전송 계층에서 웹서비스에 대한 요청 빈도를 특성으로 정의하고자 하며 이는 세션 흐름을 기록하여 패킷 수준에서 모델링함으로써 링크에서 환경적인 영향을 줄 수 있는 여러 요소(흐름 및 혼잡 제어 등)들까지 고려하고자 함이다. 많은 연구에서 웹서비스 요청 빈도는 이론적인 포아송 분포와 유사하다고 밝히고 있기에 포아송 분포를 따르는 웹트래픽은 파레토 분포에 비해 분산값이 상대적으로 작아 부하의 갑작스런 트래픽 폭주 규모가 작다고 할 수 있다[13].

또한 세션(또는 패킷, 바이트)의 분포는 모두 하루 단위로 그래프 변화가 비슷한 패턴(Time-of-Day) 특성을 나타내고 있다. 대개 오전 6시경 트래픽이 최소를 보인 뒤 점차 증가하여 오후를 지나 밤 10시경에 최고조에 달하는 현상을 보이고 있다. 이러한 특성은 대규모 네트워크에서 일반적으로 나타나는 현상으로 여러 연구결과에서 보고되고 있다[14][15].

3.1.2 응용계층 기반 특성

OSI의 최상위 계층인 응용 계층에서는 웹서비스 요청에 대한 대응하는 문서 크기를 특성으로 정의한다. 여러 논문에서 응용계층 기반 특성을 지수 분포나 정규 분포와는 달리 Heavy-Tailed 분포로써 자기 유사한 특성을 가진 파레토 분포를 좋은 웹트래픽 모델로 활용하고 있다[16]. 특히, 문서 요청 집중도는 상대적으로 크기가 작은 문서에 집중되는 Zipf(또는 Zipf-like) 규칙과 같은 분포를 보인다. 이러한 분포를 따라 생성되는 난수들의 평균과 분산이 특정 파라미터 값에 따라서는 무한한 값을 가지며 분포의 꼬리 부분에 많은 확률 값이 존재함에 기인한다. 또한, 포아송 분포에 비해 분산값이 상대적으로 크기에 부하의 갑작스런 트래픽 폭주 규모가 크다고 할 수 있다.

3.2 웹서버 가용성 향상을 위해 제안하는 동적 메커니즘

다양해지는 멀티미디어 환경에서 안정적인 웹서비스를 제공하기 위해서는 고용량, 고성능의 웹서버 시스템을 확보해야 한다. 그렇지 않을 경우 과부하 또는 심한 병목현상으로 인하여 서비스 만족도는 떨어지며 심한 경우 서비스 거부가 발생한다. 그러나 시스템 처리속도를 증가 시키고 트래픽 저장 버퍼 용량을 충분히 확보하여도 서비스 거부 공격의 돌발적인 속성인 순간적인 부하량 증가 상황에 완벽하게 대응할 수 있는 무재해 웹서버를 마련하는 것은 현실적으로 불가능하고 비용 또한 큰 문제가 아닐 수 없다.

이러한 서비스 거부 공격에 대응하기 위해서는 트래픽 부하에 따른 웹서버 자원을 적절히 조절하여 과부하 상태에 들어오는 요청에 대해서는 제한을 가하고 그렇지 않은 경우 서비스를 제공하는 동적 메커니즘이 필요하다.

3.2.1 과부하 임계치 산출

서버 과부하 시에 신속하게 과부하 상태를 극복하는 동적 메커니즘을 구현하는데 있어 과부하가 예상되는 적절한 시점을 식별할 수 있는 부하 모니터링은 필수적인 요소이다. 부하 모니터는 주기적으로 실행되면서 세션(Source IP, Destination IP, Source Port, Destination Port, Protocol ID) 수 및 트래픽 부하에 대한 통계(평균 및 표준편차 값) 등을 유지한다. 또한, 기존에 서비스 중인 연결에 대해서는 세션에 기반 한 상태 감시(Stateful Session Inspection)를 수행하여 관리·유지한다.

과부하에 대한 기준은 네트워크로 입력되는 트래픽의 부하로 기준해야 하므로 이에 대한 모델은 식(1)의 전송계층 기반 포아송 분포 수식을 활용할 수 있다.

$$p(X \le x;m) = \frac{e^{-m} \cdot m^{x}}{X!} = P \qquad (1)$$

x : 트래픽 부하량
X : 트래픽 부하량에 대한 확률변수
p : 트래픽 부하가 x 이하일 확률
P : 정상 트래픽으로 인식되어 질 수 있는 포아송 분포 누적 확률
m : 트래픽 부하 평균

관리자가 정상상태라고 설정한 범위 값(P)을 초과하는 트래픽 부하량(x)이 발생한 경우를 과부하 상태라 할 수 있으며 이 값을 비정상적인 상태로 인식할 수 있는 과부하 시점 임계값(x')으로 활용할 수 있다.

$$x' = \log_m \frac{X! \cdot P}{e^{\ m}} \quad (2)$$

이외, 다른 관점에 의해서 과부하 상태를 판단할 수 있다. 서비스 거부 공격은 웹서버의 자원을 고갈시키는 것이 목적이므로 세션을 필요로 하지 않는다. 따라서, 세션 증가량에 비해 트래픽 부하량이 수배 이상 증가 시 이 또한 과부하 상태로 인식할 수 있다. 이를 활용하기 위해 상당한 기간 동안 측정된 세션 대비 트래픽 부하량 비례값의 분포가 정규분포를 따른다고 가정하면, 세션 대비 트래픽 부하량 비례값 평균(a)과의 표준편차(σ) 거리에 의해 정상적인 또는 비정상적인 트래픽 확률 값 범위 예시를 표 1 과 같이 예측할 수 있다. 즉, 정상이 아닌 3%인(평균에서 '+'로 멀리 떨어진) 경우에 대해서 비정상 비례값으로 의도하고자 한다면 이에 해당되는 과부하 시점 임계값(x')으로 'a + 1.83σ'을 설정하면 된다.

세션 대비 트래픽 부하량을 활용한 과부하 시점 임계값은 네트워크 과부하 상태가 서비스거부공격에 의해서인지 또는 정상적인 트래픽의 폭주인지를 구분하는 침입 탐지 정확성을 높여 줄 수 있어 보안장비의 오탐율(false-positive)을 감소시켜 제품의 안전 · 신뢰성을 향상 시킨다.

3.2.2 과부하 발생 시 대응 기법

앞장에서 설정한 임계값을 기준으로 하여 웹서버 입력 트래픽 부하가 그 이상일 경우 비정상 상태 즉, 서비스거부공격으로 판단할 수 있다. 따라서 서비스 유지를 위해 적절한 대응조치가 취해져야 하는데 초창기 보안장비(예: 침입차단시스템 등)들은 과부하 시에 증적된 감사 데이터 손실방지를 위해 네트워크 자체를 차단시켰으나 이 또한 서비스거부공격과 동일한 결과를 초래하므로 추후 세션관리 기능을 강화하여 기존에 연결된 세션 트래픽만 허용하도록 개선되었다. 이는 기존 연결된 세션은 지속적인 서비스 제공으로 그 수요가 충족되지만 신규 요청 세션과 기존 세션 종료 후 재 연결에서는 서비스가 거부되어 품질 만족도를 저하시킨다. 즉, 서비스거부공격 지속 시간의 누적 분포가 10분 이내 60%, 30분 이내 80% 임을 고려하면 평균 공격 시간은 수분에서 십수분 정도 지속되기에 사용자의 서비스 신뢰도가 크게 떨어진다[13].

표 1. 산포 범위에 대한 정상적 확률 값

산포 범위	정상적 확률 값
≤+0.5σ	0.6915
≤+1σ	0.8413
≤+1.5σ	0.9332
≤+1.83σ	0.97
≤+2σ	0.9772
≤+2.5σ	0.9938
≤+3σ	0.9987

본 논문에서는 의도된 서비스거부공격으로 인한 과부하 상태 시에도 신규 요청과 기존 세션 종료 후 재 연결 세션에 대해 서비스를 제공하기 위한 동적 메커니즘을 제안한다. 이를 위해 기존에 서비스 되고 있는 기존 세션 트래픽과 신규 요청(재연결 포함) 세션 트래픽을 구분하여 처리할 수 있는 2가지 프로세스를 분리해 정의하고자 한다.

먼저, 기존 세션 처리 프로세스는 트래픽 부하가 임계값 이하일 경우에 연결된 세션을 식별 · 유지하여 임계값 이상일 경우에도 동일하게 처리한다. 이는 최소한의 서비스 품질 보장을 위한 방안으로 현재 대다수의 보안장비에서 구현된 방식과 동일하다.

이에 반해, 신규 요청 세션 처리 프로세스는 세션연결의 연결요청 대기시간(time_wait) 값을 짧게 설정 후 3 way handshake 가 완료 처리된 세션만을 유지하여 서비스를 제공하도록 한다. 이는 syn flooding 과 같은 웹서버의 자원고갈을 유도하는 서비스거부공격을 차단함과 동시에 기존 대응방법에 비해 신규 세션도 서비스 되어질 수 있는 장점이 있다.

하지만, 이러한 세션관리로 모든 신규 트래픽을 서비스 한다 할지라도 지속적으로 폭주하는 연결요청 및 세션관리 처리로 인한 노드의 컴퓨팅 파워 감소 등으로 인하여 트래픽은 다시 경쟁하게 되고 세션이 누락될 수 있어 끊김 없는 서비스 유지가 불가한 경우가 발생할 수 있다. 즉, 앞에서 설명한 바와 같이 웹서버에 대한 연결은 다수의 세션으로 이루어지므로 세션에서 하나의 문서라도 누락되거나 혹은 누락된 문서에 대한 재전송 요구로 부하가 발생할 경우 클라이언트가 느끼는 서비스의 품질 만족도는 크게 떨어진다. 따라서 낮은 품질로 모든 신규 세션에 대해 서비스를 제공하는 것보다는 제한된 수의 신규 세션에 높은 서비스 품질을 유지하는

것이 클라이언트가 느끼는 서비스 품질 만족도를 향상 시킬 수 방안이 요구되며 이에 대한 평가 지표는 다음과 같이 나타낼 수 있다.

$$\text{연결접속률}(\%) = \frac{\text{허용된 연결 수}}{\text{서비스요청 총 연결 수}} \times 100 \quad (3)$$

$$\text{연결완성률}(\%) = \frac{\text{완성된 세션 수}}{\text{허용된 연결에 의해 요구되는 총 세션 수}} \times 100 \quad (4)$$

세션 : SIP, DIP, Sport, Dport, Protocol ID 기반의 TCP 접속

연결 : 사용자가 웹서버에 요청하는 정보출력 웹페이지로 하나 이상의 세션을 필요

식 (3)의 연결접속률은 서비스를 요구한 모든 연결 중에 연결이 필요로 하는 세션 중 하나라도 접속이 허용된 연결의 비율을 나타내며 식 (4)의 연결완성률은 허용된 연결에게 필요로 하는 세션의 제공 비율을 나타낸다.

동일한 자원을 활용하여 연결접속률과 연결완성율을 높이기 위해서는, 해당 네트워크와 노드의 운영환경을 고려한 신규 웹 세션에 대한 통제 변수가 필요하다. 웹서버의 응용계층 기반 특성에 의하면 작은 크기의 문서는 서비스 집중도와 인기도가 크므로 적정 수준의 상위문서에 대해서만 선별하여 서비스 연결을 수행하도록 한다면 노드 용량이 허용하는 범위 내에서 연결 세션 수의 효율성을 높일 수 있다. 즉, 인기도가 낮고 용량이 큰 문서를 서비스 하는 것보다 인기도가 높고 용량이 적은 세션을 연결하는 것이 동일한 서비스 품질(세션에서 문서 누락 정도)을 유지하면서 더 많은 세션을 연결할 수 있는 장점이 있다. 따라서 Zipf's law는 신규 웹 세션에 대한 서비스 제공 여부를 결정하는 요소로써 차용하고자 하며 이는 적절한 설정으로 과부하의 영향을 감소시키면서 클라이언트의 요청을 처리할 수 있으므로 웹서비스에 대한 가용성을 크게 향상 시킬 수 있다. 또한, Zipf's law를 운영정책으로 활용한 예는 기존의 네트워크기반 정보보호제품(F/W, IDS, IPS, UTM, TMS 등)에서는 볼 수 없는 것이며 특히, 본 논문의 보호대상인 웹서비스의 세션 특징을 활용하기 위한 적절한 통제변수라고 생각되어진다.

3.2.3 효율성 향상을 위한 문서 서비스 최저 순위 결정

동적메커니즘 제안 배경은 그림 (2)에서와 같이 웹서버가 처리 가능한 용량이 제한되어 과부하 입력($\lambda_{net} \gg \lambda_{sys}$)에 대해 한정된 처리용량($\lambda_{sys}$)으로 모든 연결에 대한 서비스가 불가하다는 것이다. 이에 제안 방식에서는 기존 연결은 유지하여 지속적인 처리(λ_{per})를 수행하며 남은 여유 용량($\lambda_{ava} = \lambda_{sys} - \lambda_{per}$)에 대해 선택적인 서비스 분별을 위해 문서 인기도에 대한 Zipf's law 활용하고자 한다.

남은 여유 용량(λ_{ava})을 최대한 활용하면서 연결접속률과 연결완성률을 높이기 위해서는 가능한 인기도가 낮은 최저 순위값(K)이 서비스 제공여부의 임계값으로 선택되어야 하며 이 값은 앞장에서 설명된 통제변수로 설정되어야 한다. 이는 문서요청집중도는 상대적으로 크기가 작은 문서에 집중되므로

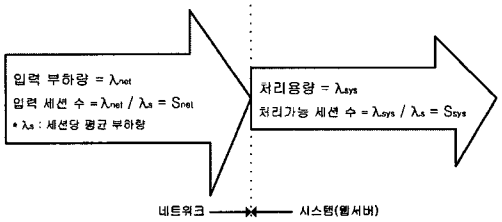


그림 2. 웹서버 및 네트워크 트래픽 환경

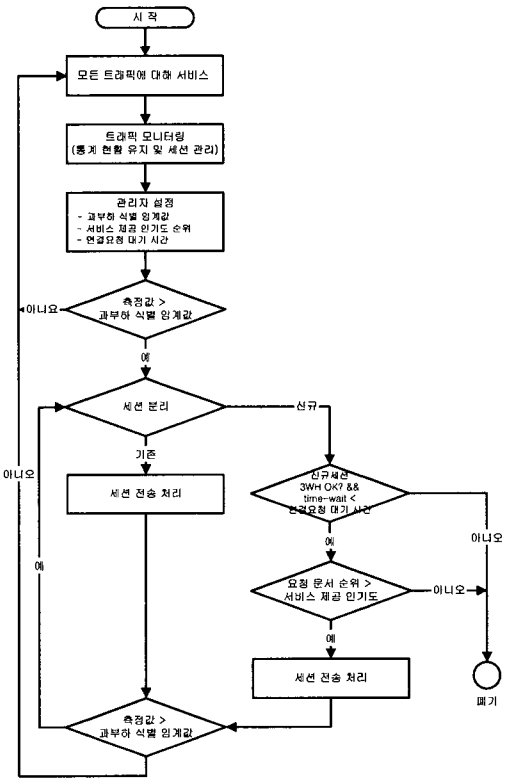


그림 3. 동적 메커니즘 프로시저

제한된 용량으로 가장 많은 세션 수를 유지할 수 있기 때문이며 그 값은 다음의 식을 만족하여야 한다.

$$\sum_{i=1}^{K} \lfloor \frac{P_i(\lambda_{net}-\lambda_{per})}{\lambda_i} \rfloor \le \frac{\lambda_{ava}}{\lambda_s} \quad (5)$$

P_i : i 번째 인기도에 대한 확률분포 값

λ_i : i 번째 인기도에 대한 평균 세션 부하량

그림 (3)은 지금까지 설명한 제안방식의 처리순서도이다.

Ⅳ. 실험 및 검토

실험 및 검토에서는 시뮬레이션을 통한 측정결과를 분석하여 서비스거부공격에 대응한 동적 메커니즘의 성능향상에 대한 근거를 제시하고자 한다.

<표 2>는 실험에서 사용될 웹서버 트래픽에 대한 통계적 특성을 나타내고 입력 원으로 사용될 웹 트래픽 통계 특성, 관리자 설정 및 환경에 대한 변수와 설정 값들을 다음과 같이 가정하여 정의하였다. 아래의 설정된 변수 값들은 보호대상 시스템의 다양한 환경에 의해 변경될 수 있는 값들로써 제한되어진다. 먼저, 웹트래픽 통계 특성 파라미터들은 정상환경에서의 평균적인 트래픽 특성을 나열하고 있으며 관리자 설정값은 보호대상 노드에 대한 웹서버의 서비스 특성을 나타내고 있으며 네트워크[시험] 환경 변수값들은 물리적 요소의 대역폭과 기존 세션에 대한 트래픽 통계적 특성을 나타내고 있다.

과부하 시점은 세션대비 트래픽량 비의 산포범위에 대한 정상적 확률값 최대치로써 동적메커니즘을 적용하기 위한 임계값으로 이 수치를 이 넘어가는 트래픽 부하량 발생 시, 기존 세션 트래픽과 신규 요청 세션 트래픽을 구분하여 기존 세션은 세션유지방식으로 기존 보안장비와 동일하게 처리하고 모든 신규 요청(재연결 포함) 세션은 Zipf's law의 통제변수에 의한 최저 문서 순위값(K)에 의해 세션이 선별적으로 서비스 되어진다.

표 2. 통계적 특성, 관리자 설정 및 환경 변수 값

웹트래픽 통계 특성	
평균세션 수	500개
평균세션 당 트래픽량	2.04K bytes
트래픽량[평균]	1M bytes
트래픽량[표준편차]	0.1M bytes

관리자 설정 값	
과부하 시점	99%
평균 연결 당 세션 수	5개
웹서버 제공 문서 갯수	1,000개

네트워크[시험] 환경	
네트워크 용량(최대 부하량)	100M bytes
시스템 용량(처리 부하량)	10M bytes
단위시간 당 세션 중단율	3%

다음으로 제안된 Zipf's law를 활용한 웹서버 대상 동적서비스 메커니즘 운영정책에 의해 궁극적으로 달성하고자 하는 바는 연결접속률과 연결완성률의 향상이며 이에 대한 공격자의 환경변수는 공격부하량과 공격지속시간으로 제한되어 진다. 이외의 변수는 위의 <표 2>에 나타낸 바와 같이 보호대상 네트워크에 대한 환경변수로 다양하고 그 값이 임의적일 수 있기에 본 논문에서 공격자 의지에 의해 달라지는 환경적 두 가지 요소에 따른 변화를 시뮬레이션을 활용한 시험대상으로 채택하고자 한다.

4.1 시간흐름에 따른 효율성 측정

제안된 동적 메커니즘에 의한 웹서비스 처리가 서비스거부공격에 적절히 대응할 수 있는지 알아보기 위해 정상적인 환경에서부터 과부하 이후의 서비스거부공격 까지의 서비스 가용성을 측정하였다. 입력 부하량 100M bytes, 평균 트래픽량 1M bytes 이상은 공격 트래픽량, 공격 패킷당 트래픽량 50bytes, 단위시간 1분 및 지속시간 100분인 실험조건하에서, 최선형 방식(과부하 시 추가적인 대응행동 없음) 및 세션 유지 방식(과부하 시 기존 연결된 세션만 서비스)과의 10회 반복된 측정을 통한 비교·분석을 수행하였다.

아래의 그림에서 나타나듯이, 제안방식은 기존의 최선형 방식 및 세션 유지 방식과 비교하여 연결접속률 및 연결완성률이 크게 향상됨을 볼 수 있다.

과부하 시 기존 방식들에 비해, 동적 메커니즘이 신규 요청(재연결 포함)세션에 대해 선별적인 통제로 자원을 최대한 활용하여 연결 세션 수가 증가된 탓으로 서비스되어 지는 세션 트래픽은 기존의 연결된 세션 외에 계산된 '서비스 최저 순위 문서 순위' 범위 안에 들어오는 상위 문서에 대한 신규 요청까지도 추가로 허용되었기 때문이다. 이는 앞장에서 서술한 제한된 자원 환경에서 인기도가 낮고 용량이 큰 문서를 서비스 하는 것보다 인기도가 높고 용량이 작은 세션을 연결하는 것이 더 많은 세션을 연결시켜 서비스 품질을 향상시킬 수 있다는 장점을 그대로 나타내고 있다.

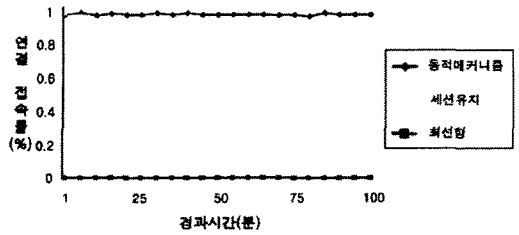


그림 4. 시간 경과에 따른 연결 접속률

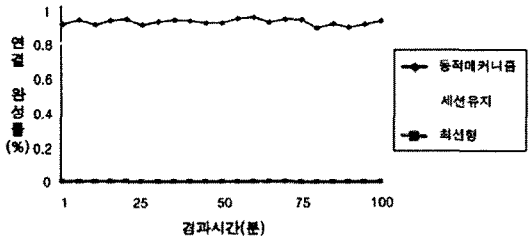


그림 5. 시간 경과에 따른 연결 완성률

4.2 서비스거부공격 부하량에 따른 효율성 측정

이번 실험에서는 서비스거부공격의 부하량 변화에 따른 제안된 동적 메커니즘의 서비스 가용성 향상을 알아보기 위해, 실험 환경을 0 byte에서부터 10M byte 까지는 1M bytes 씩 증가, 100M byte 까지는 10M byte씩 증가, 평균 트래픽량 이상은 공격 패킷, 공격 패킷당 트래픽량 50bytes 로 가정한 뒤 10회 반복된 연결접속률 및 연결완성률을 측정하였다.

제안방식은 기존의 최선형 방식 및 세션 유지 방식과 비교하여 연결접속률 및 연결완성률이 크게 향상됨과 동시에 과부하 정도에 대한 영향이 상대적으로 적음을 알 수 있으며 특히, 연결완성율은 허용된 연결에 제한되므로 제안방식은 과부하에 대한 영향이 작게 나타남을 알 수 있다. 성능향상 이유로는 기존 방식은 과부하가 가중(시스템 처리용량 10M 초과 시)될수록 확률적인 요소 또는 기존 연결세션의 처리 가능성에 의해서만 서비스가 가능하였으나 제안 방식은 과부하 발생 시 신규요청에 대한 별도의 프로세스에 의해 처리가 되어 부하량과의 관련성은 적기 때문이다. 따라서 아래 그림에서 볼 수 있듯, 연결접속률에 있어 동적 메커니즘은 과부하가 가중될수록 효과가 더욱 크게 나타나므로 다른 방식들과 대비하여 서비스 가용성이 크게 향상됨을 예상할 수 있다.

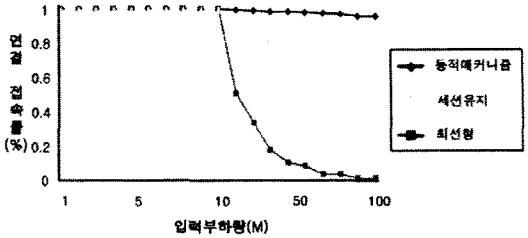


그림 6. 부하량 증가에 따른 연결 접속률

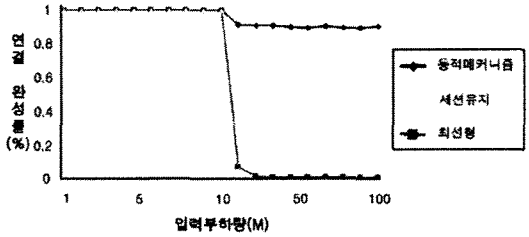


그림 7. 부하량 증가에 따른 연결 완성률

4.3 서비스 최저순위의 적절성

본론에서 정의된 통제변수인 최저 순위값이 시스템의 용량을 충분히 활용하여 서비스 가용성 높이는 임계값임을 알아 보기 위해, 입력 부하량(V_{net}) 11Mbytes, 세션처리 부하량(V_{per}) 9Mbytes 및 여유용량(V_{ava}) 1Mbytes로 가정한 뒤 연결접속률 및 연결완성률을 측정하였다.

아래의 실험결과에서 알 수 있듯, 임계값(K) '6' 부근까지 연결접속률과 연결완성률이 정점을 향해 증가함을 알 수 있으며 이는 가능한 용량이 작으면서 가장 인기 있는 문서를 선별적으로 많이 서비스 할 수 있기 때문이다. 따라서 과부하 환경에서 시스템의 용량을 최대한 활용하여 가능한 세션을 가장 많이 연결 허용할 수 있는 좋은 통제변수임을 확인하여 주고 있다.

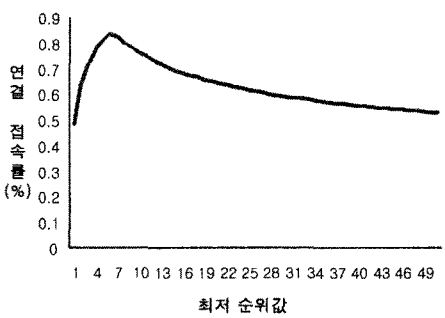


그림 8. 최저 순위값 설정에 따른 연결 접속률

V. 결 론

웹서버의 가용성을 침해하는 서비스거부공격은 정보보안과 침해영향력에 있어 가장 위협적인 존재가 아닐 수 없다. 이를 예방하기 위해 보호대상 시스템의 처리 속도를 증가시키고 트래픽 전송 및 버퍼 용량을 충분하게 확보한다고 하더라도 서비스거부공격의 돌발적인 속성으로 인해 순간적으로 가해지는 부하량 증가 상황에 완벽하게 대응할 수 있는 무재해 웹서버 구축은 불가능하며 비용 또한 큰 문제가 아닐 수 없다.

본 연구에서는 서비스거부공격에 대응하여 웹서버의 가용성을 유지할 수 있는 보안노드를 설계하고자 웹트래픽의 특성을 전송계층과 응용계층으로 분리·분석하여 과부하 시점에 대한 임계값을 도출하였고 효과적인 대응을 위해 문서 인기도에 기반한 동적 메커니즘을 제안하여 성능향상을 분석하였다. 즉, 입력되는 과부하 트래픽에 제한을 가하여 폭주 트래픽 환경 하에서도 자원의 활용도를 최대한 유지하면서 세션의 연결가능성을 극대화 시킬 수 있도록 하였다. 따라서, 자원의 활용도를 최대한 유지하여 서비스 품질 향상을 이루므로, 이는 보호대상 웹서버의 성능향상을 위해 처리 용량을 확장하는 방식이 해결하지 못한 원천적인 과부하 발생으로 인한 서비스 거부공격에 대응할 수 있다.

측정 결과, 최선형 방식과 세션유지 방식에 비해 연결접속률과 연결완성률이 크게 향상 되었으며 이는 과부하 상황에서도 신규 연결에 대한 선별적인 서비스 제공이 가능하였기 때문이다. 또한, 정의된 서비스 최저 문서 순위도 가장 효율성 높은 임계값임이 증명되었으므로 제안된 동적 메커니즘 방식은 고객의 서비스 만족도 향상에 크게 기여할 수 있으리라 생각된다.

하지만, 본 논문에서 제안한 동적 메커니즘만으로 웹서버 서비스거부공격을 완벽하게 방어하는 것은 어렵다. 서비스거부공격은 공격자의 의도에 따라 충분히 바뀔 수 있고, 다양한 방법이 지속적으로 개발되기 때문이다. 이를 위해 다양한 방어방법이 함께 적용하기를 권고되기에 본 논문에서 제안한 방법과 일반적으로 알려진 서비스거부공격 방어방법들을 이용해서 통합적인 보안시스템으로 확장해야 할 것이다.

참 고 문 헌

[1] 2007 국가정보보호백서, 국가정보원/정보통신부, 2007.

[2] Symantec 인터넷 보안 위협보고서 제10권, 2006.

[3] How to Get Rid of Denial of Service Attacks, http://www.bgpexpert.com/antidos.php.

[4] BlackHole Route Server and Tracking Traffic on an IP Network, http://www.ietf.org/rfc/rfc2616.

[5] Unicast Reverse Path Forwarding (uRPF) Enhancements for the ISP-ISP Edge, .ftp://ftp-eng.cisco.com/cons/isp/security/URPF-ISP.pdf.

[6] Internet Protocol : RFC 791, http://www.ietf.org/rfc/rfc791.

[7] Transmission Control Protocol : RFC 793, http://www.ietf.org/rfc/rfc793.

[8] QPM Command Reference, http://www.cisco.com/en/US/products/sw/cscowork/ps2064/products_user_guide_chaper09186a00800807a9.html#10134.

[9] Hypertext Transfer Protocol - HTTP/1.0 : RFC 1945, http://www.ietf.org/rfc/rfc1945

[10] Hypertext Transfer Protocol - HTTP/1.1 : RFC 2616, http://www.ietf.org/rfc/rfc2616.

[11] S. Uhlig and O. Bonaventure, "Understanding the Long-Term Self-similarity of Internet Traffic," *QOFIS2001*, Portugal, pp.286-298, Sep. 2001.

[12] Jin Cao et al., "Internet Traffic Tends To Poisson and Independent as the Load Increases," Bell Labs. Technical Report, Murray Hill, 2001

[13] Mikael Andersson, Anders Bengtsson, Martin Host, and Christian Nyberg, "Web Server Traffic in Crisis Conditions," http://www.lu.se/upload/LUCRAM/Andersson-web_server_traffic.pdf.

[14] Stefan Saroiu, Krishna P. Gummadi, Richard J, Dunn, Steven D. Gribble, and Henry M. Levy, "An Analysis of Internet Content Delivery Systems," *Proceedings of the Fifth Symposium on Operating Systems Disign and Implementation (OSDI2002)*, Boston, MA, Dec 2002.

[15] Alexandre Gerber, Joseph Houle, Han Nguyen, Matthew Roughan, and Subhabrata Sen, "P2P The Gorilla in the Cable," *National Cable & Telecommunications Association(NCTA) 2003 National Show*, Chicago, IL, Jun, 2003.

[16] Adepele, Martin Arlitt, Carey Williamson, and Ken Barker, "Web Workload Characterization: Ten Years Later," *International World Wide Web Conference(WWW2005)*, Canada, 2005

[17] (CC v2.3)국가기관용 침입차단시스템 보호 프로파일 V1.2, IT보안인증사무국, 2006.

[18] David Moore, "Inferring Internet Denial-of-Service Activity," http://www.caida.org/outreach/papers/2001/BackScatter/usenixsecurity01.pdf.

백 남 균(Namkyun Baik) 정회원

1998년 2월 숭실대학교 전자공학과 졸업

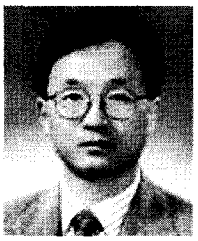
2001년 2월 숭실대학교 전자공학과 석사

2000년~현재 한국정보보호진흥원 선임연구원

2007년 3월~현재 숭실대학교 정보통신전자공학부 박사과정

<관심분야> 네트워크 보안, 보안성평가, 정보통신시스템 감사

정 수 환(Souhwan Jung) 종신회원



1985년 2월 서울대학교 전자공학과 졸업

1987년 2월 서울대학교 전자공학과 석사

1988년~1991년 한국통신 전임연구원

1996년 6월 Univ. of Washington 박사

1996년~1997년 Stellar One SW Engineer

1997년~현재 숭실대학교 정보통신전자공학부 부교수

<관심분야> 이동 네트워크 보안, VoIP 보안, 네트워크 보안, RFID/USN 보안