산업기술연구(강원대학교 산업기술연구소 논문집), 제27권 B호, 2007.
Journal of Industrial Technology, Kangwon Natl. Univ., Korea, No. 27 B, 2007.

공격자의 자원소진특성을 이용한 분산서비스불능화 (DDoS) 공격에 대한 방어

DDoS Defense Using the Exhaustiveness of Attackers

정 충 교*

Jeong, Choong-Kyo

Abstract

A novel DDoS (Distributed Denial-of-Service) defense technique, Exaustiveness-Based Detection, is proposed in this work. It dispenses with the network congestion and the unfairness between users of the Defense-by-Offense technique by incorporating a kind of simple Detect-and-Block scheme (user identification), still improving the effectiveness of the defense in comparison to the original Defense-by-Offense technique. It uses SYN cookies to identify users in the granularity of ip address and to prevent ip address spoofing by the attacker. There can be, however, some probability of false negative (denying service to good clients), if the attacker wisely adapt to the new technique by saving some portion of its bandwidth resource and later mimicking good clients. Quantitative analysis the requirement for the good clients to be safe from the false negative is provided and a procedure to design the server capacity is explained.

키워드: *분산서비스불능화, 공격, 방어, SYN 쿠키, 자원소진*
Keywords: *DDoS, attack, defense, SYN cookies, exhaustiveness*

1. 서론

서버에 대한 분산서비스불능화 (DDoS: Distributed Denial-of-Service) 공격은 공격자의 입장에서 볼 때 서버에 침입하는 것에 비해 훨씬 용이한 공격이므로 여러 가지 구체적인 기법을 통한 DDoS 공격이 빈번하게 이루어지고 있다. DDoS 공격 방법은 크게 응용 수준에서의 공격과 네트워크 수준에서의 공격으로 나눌 수 있다. 응용 수준에서의 공격은 서버를 공격할 목적으로 인위적인 서비스 요청을 서버에게 매우 많이 보내어 서버가 처리할 수 있는 한계를 초과하는 부하를 거는 기법이다. 네트워크 수준에서의 공격은 서버가 연결되어 있는 네트워크에 트래픽을 의도적으로 과다하게 발생시키거나 라우터 등 네트워크 장비의 동작을 교란시켜 네트워크 장애를 유도하고 이로 인해 서비스가 이루어지지 못하게 하는 기법이다.

이 두 가지 기법 모두 분산 방식으로 작동하는 경우가 많다. 즉 비교적 보안이 허술한 컴퓨터들 즉 개인용 컴퓨터나 실습용 컴퓨터, 대중용 컴퓨터 등에 침입하여 이들에 대한 제어권을 확보한 후 이들을 이용하여 특정 서버를 동시에 공격하는 방법을 사용한다. 그렇게 하지 않고 한 컴퓨터에서만 공격을 할 경우 자신의 위치가 드러나 쉽게 공격이 무력화되기 때문이다.

이 연구에서는 응용 수준에서의 분산서비스불능화 공격에 대한 대응 방법만을 고려한다. 네트워크

* 강원대학교 컴퓨터정보통신공학전공 교수, 공학박사

수준에서 이루어지는 공격은 응용 수준 공격과 비해 공격 수단과 대응 방법이 판이하게 다르기 때문에 전혀 다른 연구분야이다. 응용 수준에서의 분산서비스불능화 공격에 대한 대응 기술을 다시 크게 나누면, 정상적인 서버스 요청과 공격을 위한 서비스 요청을 구분하여 정상적인 서비스 요청만을 처리하는 기술[1-3]과 모든 사용자에게 사용 대가를 치르도록 함으로써 공격자가 서버스불능화 공격에 필요한 만큼의 비용을 감당하지 못하도록 하는 기술[4-6]로 분류된다. 전자는 공격탐지기법이라 할 수 있고 후자는 요금부과기법이라 할 수 있을 것이다.

공격탐지기법은 한마디로 불량사용자를 선별하는 기술이라 할 수 있다. 사용자들의 ip 주소를 관찰하여 경험적으로 불량 ip 주소를 추출해 내고 이를 기반으로 불량사용자를 골라낼 수도 있고, 정해진 수준 이상의 부하를 주는 사용자를 불량사용자로 규정하여 골라 낼 수도 있다. 또 사람만이 서비스를 사용할 수 있도록 하여 자동접속프로그램에 의한 서비스 요청을 모두 불량사용자로 판별하는 기법, 암호를 알고 있거나 특정 문제를 풀 수 있는 경우에만 정상 사용자로 인정하는 기법 등이 모두 이 범주에 든다. 이 기법에서의 핵심은 역시 판별의 정확성이다. 정도의 차이는 있지만 어느 기법을 사용하든 판별의 부정확성이 존재할 수밖에 없다.

요금부과기법은 공격자와 일반사용자를 구분하지 않고 모든 사용자에게 여러 가지 형태의 요금을 부과함으로써 공격자가 과중한 부담 탓에 충분한 공격의 효과를 얻지 못하게 하는 기법이다. 요금은 현금 등 돈이 될 수도 있고 메모리나 CPU 등 계산 부담이 될 수도 있을 것이다. 일반 (선량한) 사용자들의 요금 부담 능력의 합이 공격자의 요금 부담 능력보다 충분히 크다면 서버의 처리 능력을 적정 수준으로 초과 시설하고 적절한 요금 정책을 동원함으로써 공격의 실효성을 크게 낮출 수 있다.

이 기법은 일반사용자와 공격자의 활용가능 자원 배분이 적절한 범위 내에 있는 경우 예측 가능한 수준의 효과를 확실히 보장할 수 있다는 장점이 있다. 이는 공격탐지기법이 탐지기법의 정확도에 따라 그리고 공격자가 구현한 공격기법의 정교함에 따라 판별 오류(공격자에게 서비스를 허용하는 오류와 일반사용자의 서비스를 차단하는 오류)가 발생할 수 있다는 단점과 비교된다.

최근, 요금부과기법에 속하는 기술로서 종래에 사용하던 돈이나 계산부담이 아닌 네트워크 대역폭을 요금으로 부과하는 방안이 제안되었다 [7]. 제안자들은 이 방안을 "공격을 통한 방어"라 부르고 있다. 공격이 개시되어 서버가 서비스 요청을 모두 지원할 수 없게 되면 서버가 각 사용자에게 최대의 속도로 데이터를 보내도록 요구한다. 사용자가 보낼 데이터는 서비스 요청 메시지의 반복적인 재전송일 수도 있고, 의미 없는 임의 데이터의 전송일 수도 있다. 그러면 대부분의 일반사용자들은 지금까지 정상적으로 서비스 요청을 보낼 때에 비해 매우 많은 데이터를 서버 쪽으로 보낼 것이지만 공격자는 그렇게 하지 못할 것이다. 공격자들은 공격을 개시할 때 이미 자신이 보낼 수 있는 최대한 능력으로 서비스 요청 신호를 보냈을 것이기 때문이다.

서버는 각 클라이언트가 보낸 데이터 양에 비례하여 클라이언트에게 서비스를 제공한다. 사용자가 보내는 데이터가 서비스 요청 메시지의 반복적인 재전송인 경우에는 무작위로 일부를 선택하여 서비스를 제공하고, 사용자가 보내는 데이터가 의미 없는 임의 데이터인 경우에는 데이터의 전송량을 측정하여 그에 따라 서비스 제공 순서를 정한다. 이렇게 하면 일반사용자의 여유 대역폭 합이 공격자의 대역폭을 압도하는 경우 공격자가 차지하는 서비스 비율을 대폭 제한함으로써 서비스불능화공격을 퇴치할 수 있게 된다.

그러나 이 방안을 따를 경우 대역폭의 낭비가 심하고 사용자간 형평성에도 문제가 생기게 된다. 대역폭 낭비의 경우 사용자 접속 선로 상의 잉여 대역폭을 활용하는 것은 좋으나 서버에 대한 서비스불능화공격이 네트워크 내부의 트래픽 증가를 유도하고 이것이 네트워크 혼잡으로 이어져 다른 사용자들의 서비스 품질에 나쁜 영향을 줄 수 있다. 사용자간 형평성 문제란 공격 대응 기간 동안에는 서버가 각 사용자의 요금 부담액, 즉 각 사용자가 전송한 데이터의 양에 비례하여 서비스를 제공하므로 각 사용자는 자신의 여유대역폭에 비례하여 서비스를 차지하게 된다. 사용자가 실제로 필요로 하는 서비스 양과 그 서비스 요청을 위해 필요한 데이터 전송량이 자신의 네트워크 접속 대역폭에 비해 훨씬 작은데도 불구하고 자신의 네트워크 접속 대역폭에 비례하여 서비스를 받는 다는 것은 올바르지 않으며 불공정하다고 할 수 있다.

이 연구에서는 대역폭을 요금 부과 수단으로 삼는 "공격을 통한 방어"의 기본 아이디어를 살리되 공격탐지기법을 일부 접목시켜 네트워크 혼잡 유도 문제와 사용자간 형평성 문제를 해결하면서도 "공격을 통한 방어" 기법의 방어 능력을 더욱 향상시키는 방안을 제시한다. 대표적인 공격탐지기법은 과거 경험과 트래픽 특성 감시를 통하여 미심쩍은 ip 주소와 주소 그룹을 관리하는 ip 프로파일링이다. 이 연구에서는 ip 프로파일링보다 훨씬 단순한 기능인 사용자를 ip 주소별로 구별하는 공격탐지기법의 기초적인 방법을 사용한다.

서론에 이어 2장에서는 "공격을 통한 방어" 기

법의 내용과 문제점을 설명한다. 3장에서는 제안 아이디어를 설명하고 개별 사용자 구분을 위해 이용하는 SYN cookie에 대해 설명한다. 4장에서는 제안된 아이디어의 활용을 예를 들어 보이고 5장에서 결론을 맺는다.

2. 공격을 통한 방어 기법의 문제점

서비스불능화공격의 일반적인 과정을 정량적으로 표현하기 위해, 서버가 초당 최대 C개의 서비스 요청을 처리할 수 있다고 하고, n명의 일반 사용자들이 각각 평균적으로 초당 g개의 서비스 요청을 보내는 상황을 가정하자. 평상시 서버는 모든 일반사용자들의 서비스 요청을 모두 수용할 수 있어야 하므로 C > ng 를 만족하도록 서버 용량이 정해져 있을 것이다. 공격자는 초당 b개의 서비스 요청을 보냄으로써 서비스불능화공격을 하게 된다.

공격자가 한 사람이라고 할 때 b + ng > C 조건을 만족하도록 이 공격자가 b를 유지하면 서버 내 서비스 요청 메시지 대기열이 점점 길어지고 서비스 요청을 모두 처리하지 못하는 과부하 상태가 된다. 이 때 일반사용자들은 전체적으로 서버의 처리 능력 중 ng/(ng+b) 비율만큼만 서비스를 받을 수 있게 된다. 만약 b가 ng에 비해 매우 크다면 일반사용자가 받을 수 있는 서비스 비율은 매우 작아지며 서비스불능 상태에 가까이 가게 된다.

여기에서 서비스불능화공격을 시도하는 사람이 한 사람이라고 가정했지만 이것이 하나의 세션만을 이용해 공격이 이루어진다는 의미는 아니다. 한 컴퓨터 내에서도 여러 세션을 만들어 병렬로 서비스 요청을 대량으로 보낼 수도 있고 네트워크의 여러 곳에 흩어져 있는 많은 컴퓨터들에 bot을 심고 이들을 이용해 공격을 할 수도 있다. 어느 경우이건 공격자의 지시에 따라 시간을 맞춰 한꺼번에 공격이 이루어져야 하므로 이 모든 경우를 한사람의 공격자가 공격하는 것으로 간주한다.

"공격을 통한 방어" 기법을 사용할 경우, 공격이 개시되어 서버가 서비스 요청을 모두 지원할 수 없게 되면 서버가 각 사용자에게 최대의 속도로 데이터를 보내도록 요구한다. 그러면 모든 사용자는 자신이 보낼 수 있는 최대한 능력으로 서비스 요청 신호를 보낸다. 일반사용자는 이 때 각각 평균적으로 초당 G개의 서비스 요청을 보내고, 공격자는 초당 B개의 서비스 요청을 보낸다고 가정하자. 그림 1에 이 상황이 정리되어 있다. "공격을 통한 방어' 기법은 G는 g보다 매우 크고 B는 b보다 조금밖에 크기 않거나 같다는 성질을 이용한 것이다. 서버의 요구에 따라 각 사용자의 서비스 요청률이 변경된 후, 일반사용자가 받는 서비스 비율은 nG/(nG+B)가 된다. 만약 nG >> B이면 nG/(nG+B) ≅ 1이므로 서비스불능화공격의 효과가 미미해진다.

그러나 이렇게 할 경우 대역폭의 낭비가 심하고 사용자간 형평성에도 문제가 생긴다. 사용자 접속선로는 사용자가 독점적으로 사용하는 자원이므로 여유 대역폭을 모두 사용해도 문제가 없으나 사용자로부터 서버에 이르는 네트워크 내부 경로에 트래픽이 대폭 증가하여 혼잡 상태에 이르면 다른 사용자들의 통신 품질에 악영향을 주게 되며 이는 서비스불능화공격이 지속되는 한 계속된다. 특히 네트워크 형상 내에서 서버에 가까이 갈수록 혼잡도는 더욱 높아지고 서버 부근 전체가 혼잡 지역이 되어 네트워크 전체의 라우팅 안정성에도 나쁜 영향을 주게 된다.

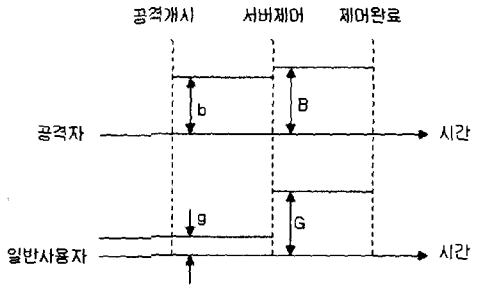

그림 1. 공격자와 일반사용자의 데이터 전송률 변화

사용자간 형평성 문제는 사용자들의 네트워크 경로 대역폭이 서로 크게 다르기 때문에 발생한다. 서비스 요청이 처리 능력을 초과하면 서버는 무작위로 선택된 요청만을 처리하므로 어느 한 사용자가 받는 서비스는 그가 보내는 요청량에 비례할 것이고 결국 큰 대역폭의 경로를 이용하는 사용자는 그렇지 않은 사용자에 비해 상대적으로 많은 서비스를 받게 된다. 이런 사용자간 불공평성은 원래 설계 목표가 아니었으며 공격 퇴치 과정에서 부수적으로 발생하는 효과이다.

3. 대역잉여율을 이용한 세션별 서비스 제어

이 절에서는 "공격을 통한 방어" 기법에서처럼 공격자가 공격을 할 때는 자기 자원의 대부분을 소진하는 상태인 반면 일반사용자는 그렇지 않다는 점을 이용하되 2절에서 서술한 "공격을 통한 방어" 기법이 갖는 문제점들을 해결한 새로운 기법을 제안한다. 제안하는 기법을 이 논문에서는

"자원소진특성판별" 기법이라고 부르기로 한다. 이 기법은 1절의 분류에 의하면 공격탐지기법과 요금부과기법의 혼합형에 해당한다고 할 수 있을 것이다. 사용자를 식별한다는 측면에서 공격탐지기법의 요소를 가지며 서비스를 받기 위해서는 충분한 대역폭을 "지불"할 수 있어야 한다는 측면에서 요금부과기법의 요소를 갖는다.

서버에 대한 서비스불능화공격이 개시되어 서버가 서비스 요청을 모두 지원할 수 없게 되면 서버가 각 사용자에게 최대의 속도로 데이터를 보내도록 요구하고 모든 사용자는 자신이 보낼 수 있는 최대한 능력으로 서비스 요청 신호를 보낸다. 서버의 요구에 따른 각 사용자의 서비스요청률의 변화(대역잉여율)를 관찰하여 그 값이 일정 기준치에 미치지 못하면 공격자로 간주하여 그 사용자에게는 서비스를 제공하지 않도록 하는 것이 "자원소진특성판별" 기법이다. 공격자 식별이 이루어지고 나면 모든 일반사용자들에게 다시 원래의 전송률로 복귀하도록 하여 정상 상태로 돌아간다.

3.1 사용자 식별 단위

이런 기법을 적용하는데 있어 중요한 설계 요소는 사용자 식별 단위를 어떻게 할 것인가이다. 세션 단위로 사용자를 식별할 것인지, ip 주소 단위로 사용자를 식별할 것인지, 아니면 사람 단위로 사용자를 식별할 것인지를 정해야 한다. 이 연구에서는 비밀번호를 사용하는 방법은 논외로 한다. 비밀번호를 사용하는 경우에는 비밀번호의 유지 관리가 핵심 과제인 반면 비밀번호만 잘 관리되면 공격에 대한 대응이 너무도 간단한 일이기 때문이다. 사람 단위로 사용자를 식별한다는 것은 비밀번호나 그에 대응되는 수단을 이용한다는 의미이므로 사람 단위로 사용자를 식별하는 방안은 논외로 한다.

세션 단위로 사용자를 식별한다는 것은 쿠키를 이용한 응용 수준의 세션을 이용해 식별하거나 TCP 연결 단위로 식별한다는 의미이다. 이렇게 할 경우에는 공격자가 한 컴퓨터 내에 여러 개의 세션을 개설하고 세션 간 데이터 전송률을 적절히 조정함으로써 서버의 대응을 무력화시킬 수 있게 된다. 즉 공격을 위해 최대한으로 요청 메시지를 보내고 있는 상태에서 서버로부터 전송률을 높이라는 요구가 오면 세션들 중 일부의 전송률은 오히려 내리고 다른 세션의 전송률을 높이는 방식으로 일부 세션을 살려 공격을 계속할 수 있게 된다.

ip 주소는 컴퓨터가 장착하고 있는 네트워크 인터페이스별로 부여되며 이 단위로 네트워크 대역폭이 결정되므로 가장 적절한 선택이다. ip 주소 단위로 사용자를 식별하여 서버의 요구에 따라 전송률이 어느 수준 이상으로 증가하지 않는 경우에는 그 ip 주소가 공격에 사용되고 있다고 판별하고 이로부터 도달하는 요청 메시지를 모두 폐기한다. ip 주소를 식별자로 사용할 수 있으려면 악의적인 사용자의 ip 위조(spoofing)를 방지할 수 있어야 한다. 공격자가 ip 위조를 할 수 있다면 ip 주소를 바꿔가면서 계속 새로운 공격을 할 수 있기 때문이다. ip 위조를 막기 위해서는 SYN 쿠키(SYN cookie)를 사용하면 된다. SYN 쿠키는 원래 네트워크 수준 서비스불능화공격인 SYN 플러딩 공격에 대한 대응책으로 개발된 것이지만 ip 위조를 방지하는 효율적이고 효과적인 방법이 되기도 한다.

3.2 SYN 쿠키

SYN 쿠키는 TCP 초기설정 과정에서 수동적으로 연결을 받아들이는 입장인 서버가 클라이언트로부터 SYN 세그멘트를 받은 후 이에 대한 반응(SYN+ACK)으로 보내는 세그멘트에 부여하는 초기순서번호(initial sequence number)이다. 원래의 TCP 구현에서는 서버가 SYN 세그멘트를 받으면 클라이언트의 ip주소와 포트번호 등 클라이언트 측에 관한 정보를 내부 큐에 저장하고 반응 세그멘트를 보냈으나 이렇게 하는 경우 SYN 플러딩 공격에 의해 미완성의 연결들이 큐를 가득 채우게 되어 서비스 불능 상태가 될 수 있다. 이런 문제를 해결하기 위해 반응 세그멘트를 보낼 때 클라이언트 쪽 정보를 내부 큐에 저장하는 대신 이 정보를 보안함수를 통해 처리하여 만들어낸 32 비트 값을 반응 세그멘트의 초기순서번호로 설정하여 보내는 방법이 제안되었는데 이것을 SYN 쿠키라고 부른다[8]. 클라이언트로부터 이에 대한 ACK 세그멘트가 도착하면 ACK의 순서번호를 확인하고 보안함수로 처리하여 쿠키를 복원하여 클라이언트 측 정보를 추출하고 연결을 완성한다.

SYN 쿠키는 이렇게 네크워크 수준의 서비스불능화공격에 대한 방어 수단으로 고안[9-12]된 것이지만 ip 위조를 방지하는 기능을 하기도 한다. 일반적으로 ip 위조를 위해서는 서버의 초기순서번호 추정이 필요하다. TCP 초기설정과정이 3단계로 구성되며 이 과정에서 상호 초기순서번호 확인이 이루어지는데 위조 ip 번호를 사용하는 클라이언트는 서버로부터 오는 반응 세그멘트를 받을 수 없고 따라서 반응 세그멘트에 들어 있는 초기순서번호를 추정하여 ACK 세그멘트를 만들고 보내야 한다. 초기순서번호는 일정한 규칙에 의해 생성되므로 공격자는 작은 노력으로 초기순서번호를 추정할 수 있으며 몇 번의 반복을 통해 초기순서번호 추정에 성공하면 바로 ip 위조가 가능해진다. 반면 SYN 쿠키를 사용하는 경우에는 클라이언트 측 정보가 보안함수를 통해 암호화된 쿠키가 초기순서

번호로 사용되므로 이를 추정하는 것이 훨씬 어렵고 따라서 ip 위조를 방지할 수 있게 된다.

3.3 분산공격과 ip공유기 (NAT, Network Address Translation)

공격자가 하나의 컴퓨터에서 공격을 하는 경우에는 공격자가 네트워크 대역폭을 최대한 이용한다는 것이 명백하다. 공격자가 여러 대의 다른 컴퓨터들을 접수하고 이들을 이용하여 분산공격을 하는 경우에는? 이 때도 공격자는 가용대역폭을 최대한 이용한다고 가정하는 것이 무리가 아니다. 물리적으로는 각 컴퓨터의 접속 대역폭에 여유가 있겠지만 공격자는 컴퓨터의 주인에게 들키지 않는 범위 내에서 몰래 작전을 수행해야 하기 때문에 보낼 수 있는 대역폭에 일정한 제한이 있게 마련이며 공격자는 이 범위 내에서만 데이터를 전송하므로 가용대역폭을 모두 소진한다는 가정에 무리가 없다.

한편 일반사용자들이 사용하는 여러 컴퓨터들이 ip공유기를 통해 네트워크에 연결될 수도 있다. ip공유기가 하나의 공중 ip번호를 사용하는 경우에는 이 컴퓨터 모두가 서버에게는 하나의 사용자로 보일 것이며 이 컴퓨터 그룹의 종합적인 잉여율은 컴퓨터 그룹의 크기와 ip공유기의 대역폭에 의해 결정된다. 지나치게 많은 일반사용자가 작은 대역폭을 갖는 ip공유기를 통해 네트워크에 연결되어 있다면 이들이 공격자로 오인되어 서비스가 거부될 수 있다. 이런 경우에 대한 정량적인 분석은 아래 소절, 자원소진특성 판별과 4절의 내용에 따라 이루어질 수 있다.

3.4 자원소진특성 판별

공격자는 일반적으로 공격을 하기 위해 자신이 동원할 수 있는 최대한의 자원을 모두 이용할 것이다. 그러므로 일반적으로는 b = B가 될 것이다. 이런 경우에는 서버가 각 사용자에게 최대의 속도로 데이터를 보내도록 요구했을 때 요청률이 증가하지 않는 사용자만 공격자로 간주하고 나머지 조금이라도 요청률이 증가하는 사용자는 일반사용자로 분류하면 된다.

그러나 자원소진특성판별기법을 사용하게 되면 공격자도 이에 적응하게 될 것이다. 즉 공격에 필요한 최소한의 자원만을 사용하고 일부 자원을 아껴 두었다가 서버의 요청에 맞춰 요청률을 올려 공격자 판별을 피하려고 할 것이다. 따라서 자원소진특성판별기법의 유효성은 공격자가 일반사용자에 비해 얼마나 많은 여유대역폭을 확보하는가에 달려있다고 할 것이다. 반면 서버는 공격자가 동원할 수 있는 최대 대역잉여율과 일반사용자가 갖는 최소 대역잉여율을 추정하고 적절한 기준값을 설정해야 할 것이다.

4. 사례 분석

공격자가 서버 혼잡을 유도하려면 b > C-ng 이어야 한다. (단, 여기에서 공격이 없는 평상시에 서비스가 원활히 이루어져야 하므로 C > ng 조건은 항상 만족해야 한다.) 그러면 공격자의 대역잉여율 B/b는 B/(C-ng) 보다 작을 것이고 일반사용자의 대역잉여율은 이보다 커야 한다. (이는 서버가 최적의 기준값을 설정한다고 가정하는 최선의 경우에 해당된다.) 서버가 초당 100개의 요청을 처리할 수 있다고 하고 (C = 100 req/sec), 공격자의 최대 전송률을 80 req/sec라고 하면, 일반사용자가 가져야 할 최소 대역잉여율은 그림 2에서 보는 바와 같다.

공격자가 확보한 최대 공격능력 G와 서버의 서비스 능력 C가 정해져 있을 때 일반사용자가 많을수록 공격자는 여유를 가지고 공격을 할 수 있게 되며 그렇게 될 수록 일반사용자가 이런 공격자와 차별성을 가짐으로써 서버가 올바른 판별을 할 수 있게 하려면 더 많은 잉여율을 확보해야 한다. 실제적으로는 일반사용자가 서비스를 거부당하는 오류기각 (false negative) 확률의 목표치를 정하고, 일반사용자들의 대역잉여율 분포와 동시에 서비스를 받는 일반사용자 수의 분포를 측정한 후, 공격자의 동원 가능한 자원 G를 추정하여, 이들을 바탕으로 서버의 필요 처리능력 C를 설계하게 된다.

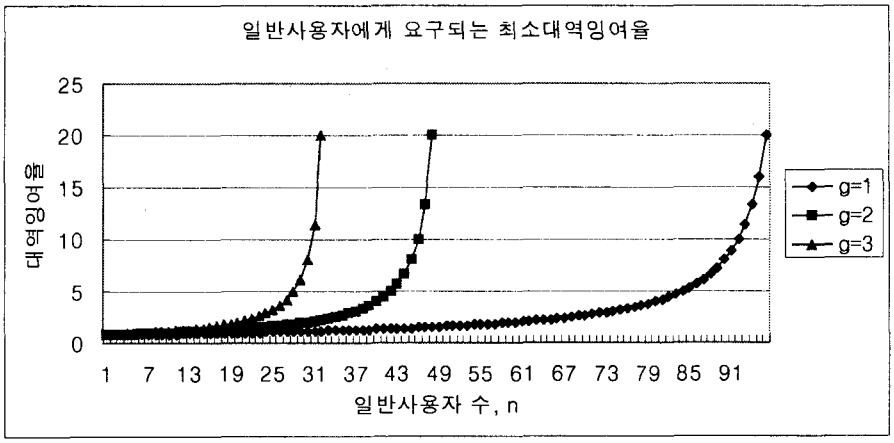

그림 2. 일반사용자에게 요구되는 최소대역잉여율 (C = 100 req/sec, B = 80 req/sec).

5. 결론

이 연구에서는 대역폭을 요금 부과 수단으로 삼는 "공격을 통한 방어"의 기본 아이디어를 살리되 공격탐지기법을 일부 접목시켜 "공격을 통한 방어" 기법에서 해결할 수 없는 네트워크 혼잡 유도 문제와 사 용자간 형평성 문제를 해결하면서도 "공격을 통한 방어" 기법의 방어 능력을 향상시키는 자원소진특성판별기법을 제시하였다. 이 기법에서는 SYN 쿠키 기술을 통해 ip 주소 단위로 사용자 판별을 하며 네크워크 혼잡 유도 문제와 사용자간 공평성 문제를 원천적으로 해결하였다. 다만 이 기법을 채택하는 경우 공격자가 이 기법에 적응하여 현명하게 공격하는 경우 어느 정도의 오류기각 확률이 존재하는데 그 정도를 정량적으로 표현하고 수치를 통해 예를 들었으며 일반적인 서버 용량 설계 방법을 제시하였다.

참 고 문 헌

[1] T. Anderson, T. Roscoe, and D. Wetherall. Preventing Internet denial-of-service with capabilities. In HotNets, Nov. 2003.

[2] Cisco Guard, Cisco Systems, Inc. http://www.cisco.com.

[3] S. Kandula, D. Katabi, M. Jacob, and A. Berger. Botz-4-sale: Surviving organized DDoS attacks that mimic ash crowds. In USENIX NSDI, May 2005.

[4] T. Aura, P. Nikander, and J. Leiwo. DoS-resistant authentication with client puzzles. In Intl. Wkshp. on Security Prots., 2000.

[5] A. Back. Hashcash. http://www.cypherspace.org/adam/hashcash/.

[6] C. Dwork, A. Goldberg, and M. Naor. On memory-bound functions for ıghting spam. In CRYPTO, 2003.

[7] Michael Walfish, Mythili Vutukuru, Hari Balakrishnan, David Karger, and Scott Shenke, "DDoS Defense by Offense, " SIGCOMM'06, September 11-15, Pisa, Italy.

[8] D. J. Bernstein. SYN cookies. http://cr.yp.to/syncookies.html.

[9] S. Bellovin. Defending Against Sequence Number Attacks. RFC 1948, May 1996.

[10] P. Ferguson and D. Senie. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoong. RFC 2267, January 1998.

[11] Livio Ricciulli, Patrick Lincoln, and Pankaj Kakkar. TCP SYN Flooding Defense. In Comm. Net. and Dist. Systems Modeling and Simulation Conf. (CNDS' 99), 1999 Western MultiConf. (WMC' 99),, San Francisco, CAL, USA, January 1999.

[12] Eric Schenk. Another new thought on TCP SYN attacks, 1996. http://www.wcug.wwu.edu/lists/netdev/199609/msg00115.html.