네트워크 기반 서비스 거부 공격에 대응한 가용성 유지를 위한 보안 노드 분석 및 설계

정회원 백 남 균*, 김 지 훈*, 신 화 종*, 이 완 석*

An analysis and design on the security node for guaranteeing availability against network based DoS

Nam-Kyun Baik*, Ji-Hoon Kim*, Hwa-Jong Shin*, Wan-Suck Yi* ***Regular Members***

요 약

본 연구에서는 네트워크 기반 서비스 거부 공격에 대응하여 허용된 서비스 거부확률을 보장할 수 있는 적합한 네트워크 노드를 설계하기 위해, 보호 대상 시스템 상위 노드 단의 상위 준위와 하위 준위의 물리적인 전송 대역, 버퍼 용량, 네트워크 기반 서비스 거부 공격에 소모된 자원, 허용 가능한 공격 소스 수 및 손실 확률에 대한 관계를 분석한 제한 조건을 도출하였고 이에 대한 네트워크 노드의 자원과 비용의 관계를 분석하여 보장된 가용성을 유지할 수 있는 경제적 노드의 자원 구성을 설계하였다.

따라서 본 연구 결과는 네트워크 기반 서비스 거부 공격에 대응할 수 있는 효율적인 보안 네트워크 구조 설계에 기여할 것으로 기대된다.

Key Words : Network based DoS, ON-OFF Model, Effective Bandwidth, Cost Function, Loss probability

ABSTRACT

In order to design network node for guaranteeing availability against network based DoS attack, some restrictions such as the relationship analysis on upper and lower layer bandwidth, buffer capacity, attack resources, a number of attack session and loss probability are analyzed. And then, to make good use of network resource, the relationship between required resources for satisfying loss probability and cost is discussed.

The results of this study are expected to be applied to the effective security node design against network DoS.

Ⅰ. 서 론

인터넷 환경의 급속한 확장 및 보급으로 각종 통신망은 시간과 장소에 제약을 받지 않고 다양한 정보를 공유할 수 있도록 네트워크를 형성하여 전세계가 하나로 상호 연결되어 있다. 이러한 정보화의 가속화는 정보 시스템을 통한 정보 제공 서비스 등으로 필요한 정보를 공유할 수 있는 혜택을 주는 반면 각종 통신망을 통하여 개인 및 사회의 중요한 정보에 대한 불법적인 침입 및 공격 등의 역기능에 처해 있다.

과거에는 단순히 특정 시스템의 버그 및 공개된 취약점에 대한 공격이 주류를 이루었다. 그리고 좀 더 나아가 침입차단시스템, 침입탐지시스템 및 기타 보안시스템을 우회하기 위한 좀더 진보된 종류의 공격들이 나타났다. 하지만 근래에는 백오리피스로 대표되는 트로이잔(trojan), 인터넷 웜(worm) 및 백도어(backdoor) 형태의 공격이 많이 등장하고 있

* 한국정보보호진흥원 산업지원단 평가 2팀
논문번호 : 030302-0722, 접수일자 : 2003년 7월 22일

으며, 이중 네트워크 자원에 대한 가용성을 침해하는 서비스 거부 공격은 공격도구의 분산화(distributed), 에이전트화(agent), 자동화(automation) 그리고 은닉화(stealth)된 특징 등으로 인하여 정보 보안과 침해영향력에 있어 가장 위협적인 존재가 아닐 수 없다. 또한 네트워크 기반 서비스 거부 공격은 침입경로의 다양성 및 수집된 로그 분석의 한계·난해성으로 인하여 실시간 분석이 불가능할 뿐 아니라, 위조된 주소 사용으로 인하여 근원지를 추적하여 적절한 대응조치를 통한 추가 피해에 대한 예방에 있어 아직 뚜렷한 현실적인 해결책이 없는 실정이다. 이에 본 연구에서는 네트워크 서비스 거부 공격에 대응하여 허용된 서비스 거부 확률을 보장할 수 있는 네트워크 노드를 설계하기 위해, 보호 대상 시스템 상위 노드 단의 상위 준위와 하위 준위의 물리적인 전송 대역, 버퍼 용량, 네트워크 기반 서비스 거부 공격에 소모된 자원, 허용 가능한 공격 소스 수 및 손실 확률에 대한 관계를 분석한 제한 조건을 도출하였고 이에 대한 네트워크 노드의 자원과 비용의 관계를 분석하여 보장된 가용성을 유지할 수 있는 경제적인 네트워크 노드 설계에 대한 구성 요소를 분석·논의 하고자 한다. 또한, 본 논문의 목적은 네트워크 기반 서비스 거부 공격에 대한 능동적 대응책이라기 보다는 수동적 방어책에 대한 보안 네트워크 노드 분석 및 설계를 목적으로 한다.

본 논문의 구성은 다음과 같다. 2 장에서는 서비스 거부 공격의 분류와 함께 각각의 공격 방식 및 특징을 먼저 기술한다. 3 장에서는 최악의 경우 모델에 의한 네트워크 가용성 유지를 위한 대역폭 할당 방법 및 트래픽 손실 확률에 대해서 논의하고 4 장에서 망 구성 비용 요소를 고려한 비용 함수를 정의하며 5 장 실험 및 검토에서는 서비스 가용성 유지를 위한 손실 확률과 노드 구성 방식에 따른 구축 비용과의 상관관계를 알아보며 7 장에서 마지막으로 결론을 정리한다.

Ⅱ. 서비스 거부 공격

2.1. 시스템 기반 서비스 거부 공격

일반적인 서비스 거부 공격은 시스템에 대한 정상 서비스를 방해하는 것이다. 즉, 네트워크 대역폭을 고갈시키는 공격이 아니라 시스템의 서비스 구성요소 즉, 시스템 자원 및 예외처리 오류 등에 대하여 공격을 수행함으로써 결국 제공되는 서비스를 저해하거나 잃어버리게 하는 것이다. 이러한 공격에 대한 구분은 표 1과 같이 크게 3가지 형태로 나눌 수 있다.

표 1. 시스템 기반 서비스 거부 공격 유형

구분	공격 방법
파괴 공격	디스크 파티션 포맷팅, 시스템 파일 삭제 등 핵심 서비스 지원 요소를 제거함으로서 서비스 기능을 상실하게 하는 공격
과부하 공격	버퍼오버플로우, 플루딩 등 시스템의 자원을 소모함으로서 서비스 기능을 상실하게 하는 공격
불완전성 공격	TCP/IP 스택의 취약성, 비정상 패킷처리의 예외 상황 등 시스템 처리루틴의 부재로 인하여 서비스 기능을 상실하게 하는 공격

시스템 기반 서비스 거부 공격의 또 다른 큰 특징은 공격자의 신분을 숨기기 위해서 위조된 근원지 주소 사용과 분산공격이 아닌 하나의 시스템이 다른 시스템을 공격한다는 것이다.

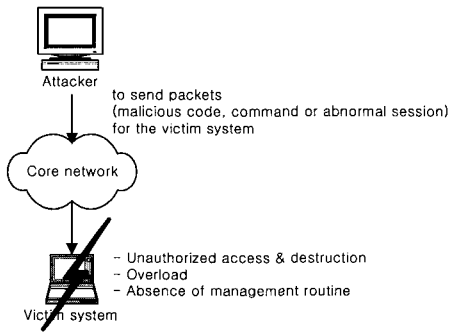


그림 5. 시스템 기반 서비스 거부 공격

2.2. 네트워크 기반 서비스 거부 공격

인터넷 상에서 컴퓨터나 네트워크는 라우터에 의해서 통신 서비스를 수행하게 된다. 종단 라우터는 ISP(Internet Service Provider) 네트워크의 고객 가장자리(customer edge)에 위치하고 작은 규모인 고객 네트워크의 트래픽을 모으고 분산한다. 따라서 인터넷으로 연결되어 네트워크간 통신을 위한 라우팅을 하기 위해서는, 대역폭이 작은 수많은 네트워크들이 하나의 높은 대역폭을 가지는 네트워크로 집결된다. 즉, 상위준위의 "Big Pipe"로 인터넷 트

랙픽이 유입되어 저장되고 대역폭이 낮은 하위준위의 여러 "Small Pipe"들한테 분리하여 전송한다. 그러나, "Big Pipe"가 단일 목적지로 향하는 패킷 흐름으로만 채워진다면, 다른 목적지로 향하는 많은 패킷들이 처리용량 한계로 인하여 고의로 버려지게 된다. 즉, 다른 목적지를 가지고 "Small Pipe" 네트워크 자원에 접근을 시도하는 클라이언트가 정상적인 패킷을 보내게 되더라도 패킷을 잃게 되고 버려진 패킷을 다시 전송하게 될 것이다. 그러나, 클라이언트는 일반적으로 몇 번의 시도 후에는 포기할 것이며 그로 인하여 회생자 서버에 의한 서비스를 제공받지 못하게 된다.

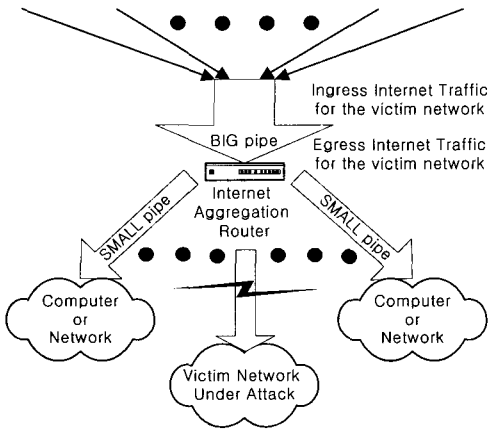


그림 2. 네트워크 기반 서비스 거부 공격 (대역폭 고갈)

네트워크 기반 서비스 거부 공격은 회생자 서버의 네트워크 연결 대역폭 자원을 고갈시키기 위해 악의의 의미 없는 인터넷 트래픽을 생성한다. 악의의 패킷들은 네트워크상에서 정상적인 서비스 트래픽과 경쟁하게 되고 최선형(best effort) 연결 방식과 종단 라우터의 상·하위 준위간의 대역폭 차이에 의해서 결과적으로 유효한 패킷들이 흐름에서 살아남을 가능성이 낮아지는 것이다. 따라서, 서버와 클라이언트간의 서비스 패킷이 교환되지 않으므로 정상적인 서비스의 유지가 불가능하다.

다음 장에서는 네트워크 기반 서비스 거부 공격에 대응하여 가용성을 유지할 수 있는 효율적인 보안 네트워크 노드 설계를 위하여 먼저, 현재 널리 악용되어 지고 있는 분산 서비스 거부 공격과 분산 반사 서비스 거부 공격의 개요를 알아본다.

2.2.1. 분산 서비스 거부 공격 (DDoS : Distributed Denial of Service)

분산 서비스 거부 공격은 많은 수의 호스트들(이미 침해되어진)에 패킷을 생성시킬 수 있는 공격용 에이전트 프로그램들이 분산 설치되어 이들이 서로 통합된 형태로 선택된 희생자 시스템(네트워크)에 대하여 일제히 악의적 데이터 패킷을 범람시켜서 네트워크 병목현상의 혼잡을 통한 패킷 손실을 유도하는 방식이다.

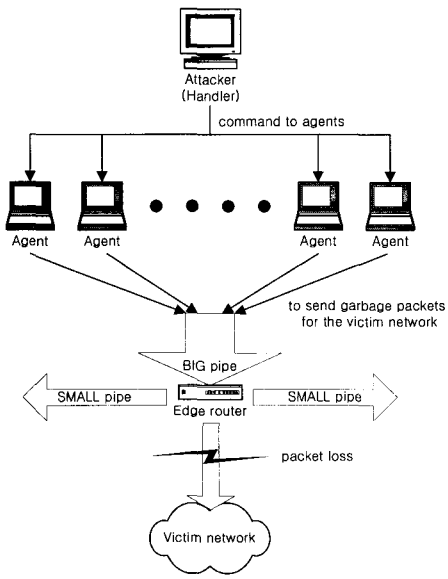


그림 3. 분산 서비스 거부 공격 구조도

그림 3 에서 나타나는 구조는 일반적으로 분산 서비스 거부 공격에서 사용된다. 원격으로 조정되는 공격(zombie) 프로그램이 설치되어 있는 에이전트 시스템은 중앙 조정 센터(central control agency)인 핸들러에 의해 공격을 지시 받게된다. Zombies 네트워크가 공격지시를 받으면 하나의 희생자 머신이나 네트워크를 목표로 하는 악의적인 트래픽 흐름(a flood of malicious traffic)을 생성하기 시작한다. 흐름이 마지막으로 희생자의 ISP 라우터를 만나게 되면 네트워크 트래픽의 대부분이 버려지게 된다. 라우터는 유효한 트래픽과 유효하지 않은 트래픽을 구분할 수 없기 때문에 (라우터는 모든 패킷을 동일하게 처리) 네트워크의 유효한 트래픽 또한 버려지게 될 것이다.

시스템 기반 서비스 거부 공격과 비교한 분산 서비스 거부 공격의 특징은 다음과 같다.

· 분산화(distributed)
· 에이전트화(agent)
· 자동화(automation)
· 은닉화(stealth)

2.2.2. 분산 반사 서비스 거부 공격 (DRDoS : Distributed Reflection Denial of Service)

2002년 1월 11일 grc.com 에서 최초 발견된 분산 반사 서비스 거부 공격은 좀 더 진일보한 악의적인 패킷 흐름을 생성하는 공격으로 인터넷 상에 접속 가능한 모든 TCP 서버들(반사서버목록(RSL) : Reflection Server List)을 에이전트로 이용할 수 있으며 선택된 서버 목록에 대해서 출발지가 위조된 SYN 패킷을 보냄으로서 각 서버들은 위조된 주소로 SYN/ACK 패킷으로 희생자 시스템에 응답한다. 희생자 시스템은 ACK 응답을 수행하지 않으므로 서버는 패킷 손실로 가정하여 재전송을 수행함으로 자연스럽게 초기에 보낸 SYN 패킷수 보다 SYN/ACK 패킷은 운영체제별 TCP/IP 스택의 재전송 방식에 의한 설정 횟수 배만큼 증가하여 네트워크 대역폭을 고갈시키게 한다. 즉, 분산 서비스 거부 공격이 여러 서버에 설치된 특정 에이전트에 의해 공격이 진행되는 반면 분산 반사 서비스 거부 공격은 정상적인 서비스를 운영하고 있는 서버를

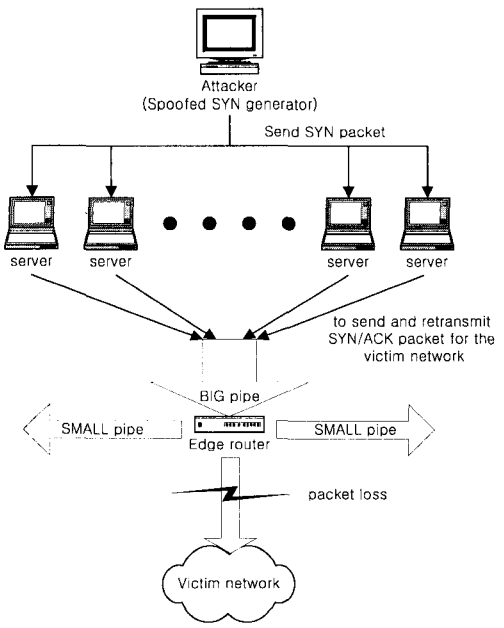


그림 4. 분산 반사 서비스 거부 공격 구조도

에이전트로 활용하기 때문에 공격자들이 손쉽게 이용할 수 있다. 또한, 공격의 근원지를 추적하기 어렵고 공격을 막을 수 있는 방법이 그리 쉽지 않으며 정상적인 인터넷 상의 서버를 활용함으로 능동적 대응 또한 용이하지 않다.

분산 서비스 거부 공격과 비교한 분산 반사 서비스 거부 공격의 특징은 다음과 같다.

· 패킷경로확산(packet path diffusion)
· 반사서버의 단계적 대응
(reflector usage phasing)
· 반사서버 확산(reflector diffusion)
· 대역폭 증대(bandwidth multiplication)
· 개선된 관리(improved manageability)

Ⅲ. 네트워크 가용성 유지를 위한 대역폭 할당

3.1. 종단 라우터 구조

앞장에서 설명한 바와 같이 유효한 패킷 손실 원인은 근본적으로 백본망인 종단 라우터의 상위 준위(λ_{upper} : Big Pipe)와 가입자망인 하위 준위(λ_{lower} : Small Pipe)간의 물리적인 전송대역의 차이에 따른 버퍼오버플로우에 의해 그림 5와 같이 종단 라우터 내장 버퍼의 입력단 위치에서 발생한다.

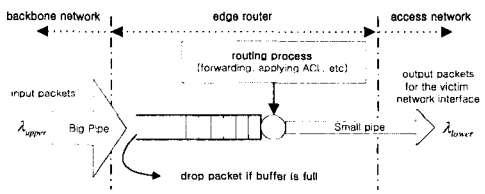


그림 5. 종단 라우터 구조 및 패킷 손실 지점

3.2. 단일 소스에 대한 손실 없는 서비스를 위한 유효 대역폭

네트워크 대역폭 고갈 공격에 대응하여 시스템의 정상적인 서비스를 유지하기 위해서는 비정상 공격 세션 트래픽을 수용할 수 있는 유효대역폭(effective bandwidth)을 알아야 한다[11]. 보호 대상 시스템에 대한 종단 라우터의 하위 준위 대역폭과 내장 버퍼 용량만을 알고 있는 경우, 지연을 고

려하지 않은 트래픽 손실이 없는 서비스 가용성을 보장하는 유효대역폭을 구하기 위해서는 공격 소스에 의해 종단 라우터로 유입되는 트래픽에 대하여 최악의 경우로 모델링해야 한다[2]. 이러한 최악의 경우 모델로는 NEC 와 Lucent 에서 자원 할당 및 호 수락 제어의 소스 모델로 사용하고 있는 ON-OFF 모델이 있으며 그림 6과 같이 트래픽이 최대 입력률로 들어오는 상태(ON-state)와 발생하지 않는 상태(OFF-state)로 일반화 될 수 있다[3][4].

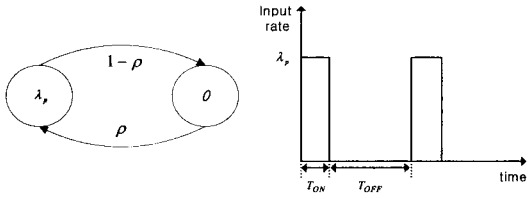


그림 6. ON-OFF 최악의 경우 모델

λ_p : 최대 입력 트래픽율

ρ : 주기에서 최대 입력 트래픽율로 유입되는 시간 비율

T_{ON} : 주기에서 최대 입력 트래픽율로 유입되는 시간

T_{OFF} : 주기에서 트래픽이 발생되지 않는 시간

ON-OFF 최악의 경우 모델에 대한 각 상태의 점유 시간은 다음과 같이 표현될 수 있다.

$$T_{ON} = \frac{B_s}{\lambda_p}$$

$$T_{OFF} = B_s(1/\lambda_s - 1/\lambda_p) \quad (1)$$

λ_s : 평균 입력 트래픽율

B_s : 주기에서 입력 트래픽의 최대 burst 크기

따라서, ON-OFF 최악의 경우 모델을 사용한 손실 없는 경우의 유효 대역폭(λ_e)과 버퍼(b)의 관계식은 다음의 식으로 표현될 수 있다.

$$b = \frac{B_s}{\lambda_p}(\lambda_p - \lambda_e) \quad , \quad [\lambda_s \leq \lambda_e \leq \lambda_p]$$

$$\lambda_e = \lambda_p(1 - \frac{b}{B_s}) \quad (2)$$

참고적으로, 식 (2)에 의해서 보장되어지는 최대 지연 시간($D_{\max}$)은 주어진 버퍼를 산출된 유효대역폭으로 나눈 값으로 다음의 식 (3)과 같다.

$$D_{max} = \frac{b}{\lambda_e} \quad (3)$$

3.3. 집합된 소스에 대한 손실 없는 서비스를 위한 유효 대역폭

네트워크 기반 서비스 거부 공격에서, 분산된 에이전트들에 의해 생성되는 공격 소스 트래픽들은 동일한 트래픽 특성을 가진다. 따라서 독립적인 N 개의 비정상 공격 세션 트래픽이 종단 라우터에서 다중화 되어 서비스 될 경우, 집합된 비정상 공격 세션 트래픽에 대응하여 손실 없는 서비스를 제공하기 위해 필요한 버퍼 용량(b_{total})과 서비스 대역폭(λ_{total})은 fluid flow approximation 에 의해 다음의 식으로 표현된다[5].

$$b_{total} = \sum_{i=1}^{N} b_i = N \times b$$

$$\lambda_{total} = \sum_{i=1}^{N} \lambda_{e_i} = N \times \lambda_e \quad (4)$$

이와 반대로, 고정된 버퍼 용량과 서비스 대역폭에 대하여 손실 없는 서비스를 제공하기 위한 허용 가능한 공격 소스 수(C_{noloss})는 출력단 대역폭을 비정상 공격 세션 트래픽의 유효대역폭($\lambda_{e(attack)}$)으로 나누어 식 (5)와 같이 구할 수 있다.

$$C_{noloss} = \lfloor \frac{\lambda_{lower}}{\lambda_{e(attack)}} \rfloor \quad (5)$$

3.4. 비정상 공격 세션 트래픽에 의한 패킷 손실 확률

그림 5와 같이 종단 라우터에서의 패킷 손실로 인한 서비스 거부는 내장 버퍼의 입력단 위치에서

발생한다. 하위 준위 대역폭의 일상적인 평균 트래픽 사용량을 λ_{usage} 라 하면, 비정상 공격 세션 트래픽에 의해 손실이 발생하는 시점은 하위 준위 대역폭에서 평균 트래픽 사용량을 제외한 평균 잉여 대역폭($\lambda_{surplus}$)에 대해서 허용 용량 이상의 트래픽이 유입되는 경우(패킷 손실을 유발하는 최소 공격 소스 수($C_{lossstart}$)로 식 (6)과 같다.

$$C_{lossstart} = \left\lfloor \frac{\lambda_{lower} - \lambda_{usage}}{\lambda_{e(attack)}} \right\rfloor = \left\lfloor \frac{\lambda_{surplus}}{\lambda_{e(attack)}} \right\rfloor \quad (6)$$

네트워크 기반 서비스 거부 공격에 의한 비정상 공격 세션 트래픽은 동일한 특성을 가진 트래픽을 발생시키므로, 잉여대역폭에 대한 패킷 손실 확률(P_{loss})은 식 (7)과 같이 나타낼 수 있으며 패킷 손실을 유발하는 최소 공격 소스 수($C_{lossstart}$) 이상으로 공격 시도(N) 시에 손실이 발생할 수 있는 확률 총합의 최대치이다. 즉, 최악의 경우로 다중화 시 트래픽이 입력되는 상태(ρ)가 겹쳐지는 확률 분포는 이항 분포를 따르므로 실제 비정상 공격 소스 트래픽에 대한 손실 확률은 최악의 경우보다 작거나 같다[6].

$$P_{loss} = \sum_{C_{lossstart}}^{N} \left[\binom{N}{C_{lossstart}} \rho^{C_{lossstart}} (1-\rho)^{N-C_{lossstart}} \right] \quad (7)$$

Ⅳ. 비용 함수

망 구성 비용에 영향을 미치는 요소들은 매우 다양하다[7]. 따라서 모든 망 구성 비용 요소를 고려하여 계산하는 것은 매우 어렵고 복잡하며 많은 시간을 요하므로, 본 논문에서는 망 구성 비용 중 종단 라우터의 버퍼용량, 내부 입출력 대역폭 및 하위 준위의 선로 대역폭에 대한 버퍼와 선로 비용만을 고려하고자 한다.

4.1. 선로 비용

망의 전송 대역(λ_{link})이 증가함에 따라서 대역폭 당 가격은 감소한다고 가정한다. 선로 구성에 드는 고정 비용을 a_1이라고 하고 전송 속도에 따른 가격 상승분을 a_2라고 하면 식 (8)과 같이 망 선로 당 가격(C_{link})을 결정할 수 있다.

$$C_{link}(\text{비용/선로}) = a_1 + (a_2 \times \lambda_{link}) \quad (8)$$

4.2. 버퍼 비용

버퍼는 트래픽을 저장할 수 있는 메모리의 집합으로 생각할 수 있으므로 우선 메모리의 가격을 결정하여 이들의 대수적인 합으로 버퍼의 총 비용을 결정할 수 있을 것이다. 가격을 결정하는 요소로 내부 대역폭과 메모리의 용량만을 고려하였고 버퍼의 비용도 망 선로 비용과 마찬가지로 버퍼용량(V)이 증가하고 내부 입출력 대역폭이 증가할수록 저장용량과 내부 입출력 대역폭 당 가격은 감소한다고 가정한다. 기본적으로 버퍼를 설치하는데 드는 비용을 b_1이라 하고 저장 용량에 대한 대역폭 당 가격 상승분을 b_2라고 하면 버퍼 당 가격은 식 (9)와 같다.

$$C_{buffer}(\text{비용/버퍼}) = b_1 + (b_2 \times V \times \lambda_{buffer}) \quad (9)$$

4.3. 망 구성 비용

망 구성 비용(C_{total})은 망 선로 비용과 망 버퍼 비용의 합으로 생각할 수 있으므로 식 (10)을 망 구성을 위한 전체 비용 함수로 정의하였다.

$$C_{total} = C_{link} + C_{buffer} \quad (10)$$

Ⅴ. 실험 및 검토

실험 및 검토에서는 시뮬레이션을 통한 측정 결과를 분석하여 네트워크 기반 서비스 거부 공격에 대응하여 허용된 서비스 거부 확률을 보장할 수 있는 경제적인 노드 설계에 대한 근거를 제시하고자 한다.

표 2는 실험에서 입력원으로 사용될 비정상 공격 세션 트래픽 소스에 대해서 가정된 정의와 이에 따른 통계적 특성을 나타낸다.

표 2. 입력원으로 사용될 가정된 비정상 공격 세션 트래픽의 통계적 특성

	평균 입력 트래픽률 (λ_s)Mbps	최대 입력 트래픽률 (λ_p)Mbps	입력 트래픽의 최대 burst 크기 (B_s)bits	주기에서 최대 입력 트래픽율으로 유입되는 시간 비율 (ρ)%
공격 소스	0.01	0.08	400	20

집합된 비정상 공격 세션 트래픽들에 대해서 손실 없는 서비스를 보장하는 유효 대역폭을 구하기 위한 시뮬레이션에서는 버퍼크기를 10K로 고정하고 집합되는 공격 소스 수에 따른 유효대역폭을 측정하여 그림 7에 나타내었다. 식 (2)와 (4)에서 알 수 있듯 집합된 공격 소스 수가 증가할수록 필요한 유효대역폭은 선형적으로 증가함을 볼 수 있다.

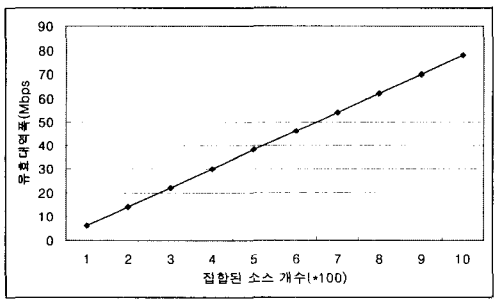


그림 7. 집합된 공격 소스들에 의한 유효 대역폭

하위 준위의 대역폭 변화에 따른 공격 소수 수에 의한 손실을 유발하는 최소 공격 소스 수를 구하기 위한 시뮬레이션에서는 버퍼크기를 100K, 하위 준위 대역폭에 대한 일상적인 평균 트래픽 사용량을 4Mbps 및 상위 준위 대역폭은 무한대로 가정하였다.

위의 가정사항에 대해, 하위 준위의 대역폭 변화에 의해 손실을 유발하는 최소 공격 소스 수는 식 (5)와 (6)에 의해 대역폭이 증가할수록 잉여대역폭이 증가하므로 선형적으로 증가함을 표 3을 통하여 알 수 있다. 따라서 계산되어진 잉여 대역폭으로, 예상되는 비정상 공격 세션 트래픽에 대해서 손실 없는 서비스를 보장할 수 있는 최대 공격 세션의 수를 계산할 수 있다.

표 3. 손실을 유발하는 최소 공격 소스 수

	하위 준위 대역폭(Mbps)					
	10	12	14	16	18	20
손실을 유발하는 최소 공격 소스 수	76	101	126	151	176	201

고정된 하위 준위 대역폭에 대한 공격 소스 수에 의한 손실 확률을 구하기 위한 시뮬레이션에서는 버퍼크기를 100K, 하위 준위를 10Mbps, 하위 준위 대역폭에 대한 일상적인 평균 트래픽 사용량을 4Mbps, 잉여대역폭을 6Mbps 및 상위 준위 대역폭은 무한대로 가정하였다.

식 (7)에 의해 공격 소스 수가 증가할수록 잉여대여폭에 대한 공격 트래픽의 점유율 증가로 인하여 손실 확률이 증가함을 표 4에 의해 알 수 있다. 위의 가정사항에 대해, 공격 소스 수가 300개를 넘는 시점부터 가시적인 손실이 발생하며 500개 이상에서는 거의 100%에 가까운 손실 확률을 보인다.

표 4 공격 소스 수에 따른 손실 확률

		손실 확률
공격 소스 수	50	0
	100	3.08588e-33
	150	6.12475e-17
	200	3.34903e-9
	250	6.19143e-5
	300	0.0143961
	350	0.229316
	400	0.710153
	450	0.958521
	500	0.997617

하위 준위의 대역폭 변화에 따른 공격 세션 수에 의한 손실 확률을 구하기 위한 시뮬레이션에서는 버퍼크기를 100K, 하위 준위를 10Mbps, 하위 준위 대역폭에 대한 일상적인 평균 트래픽 사용량을 4Mbps, 잉여 대역폭을 6Mbps, 공격 세션 수를 200개 및 상위 준위 대역폭은 무한대로 가정하였다.

위의 가정사항에 대해, 할당된 대역폭이 증가할수록 비정상 공격 세션 트래픽을 수용할 수 있는 잉여대역폭이 증가하므로 하위 준위의 대역폭 증가에 따라 손실 확률이 감소함을 표 5를 통하여 알 수 있

다. 따라서, 서비스 가용성 유지를 위한 손실 확률을 보장할 수 하위 준위 대역폭을 구할 수 있다.

표 5. 하위 준위 대역폭에 의한 손실 확률

	하위 준위 대역폭(Mbps)					
	10	12	14	16	18	20
손실 확률	0.997617	0.473272	0.0027152	3.98401e -8	1.88739e -15	4.05565e -25

이번 시뮬레이션에서는 표 6에 의한 가격 구성에 대해서 두 가지 경우에 의한 노드 구축 비용을 구하고자 한다.

표 6. 비용함수 할당치

	선로 비용 함수			버퍼 비용 함수			
	고정 비용	가격 상승분	선로 대역폭 단위	고정 비용	가격 상승분	버퍼 용량 단위	내부 입출력 대역폭 단위
할당치	100	10	1M	100	10	100K	1M

100K 버퍼 크기, 내부 입출력 대역폭 10Mbps 및 선로 대역폭 10Mbps 용량을 수용하는 노드에 대한 구축 비용 계산을 위한 첫 번째 경우에서는 1M 선로 대역폭을 가진 선로 다수개와 1M 내부 입출력 대역폭으로 10K 버퍼 크기를 가진 버퍼 다수개로 노드를 구성하며 두 번째 경우에서는 10M 선로 대역폭을 가진 선로 유일개와 10M 내부 입출력 대역폭으로 100K 버퍼 크기를 가진 버퍼 유일개로 노드를 구성하는 경우이다.

식 (8), (9) 및 (10)에 의해서 계산된 결과를 그림 8에 나타내었다. 적용된 식에 의해 쉽게 예상할 수 있듯 각 비용함수별 고정비용과 용량에 따른 가격 상승분에 의해, 대용량 선로 및 버퍼를 사용하여 노드를 구축하는 경우가 저용량 선로 및 버퍼들에 의한 구성 보다 훨씬 경제적임을 알 수 있다. 또한, 이번 시뮬레이션을 통하여 서비스 가용성 유지를 위한 손실 확률과 노드 구축 비용과의 상관 관계를 알 수 있으므로 이를 이용하여 예산된 구축 비용과 목적된 서비스 품질에 따른 경제적인 노드 설계 및 구축에 활용할 수 있다.

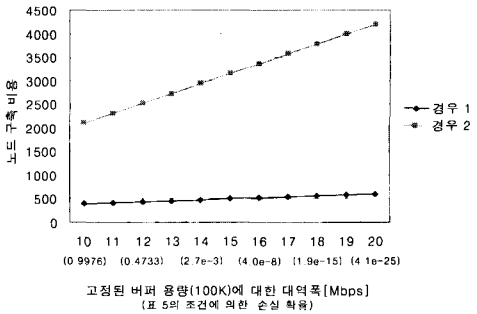


그림 8. 대역폭 변화에 따른 노드 구축 비용

VI. 결 론

본 연구에서는 네트워크 기반 서비스 거부 공격에 대응하여 허용된 서비스 거부확률을 보장할 수 있는 적합한 네트워크 노드를 설계하기 위해, 보호 대상 시스템 상위 노드 단의 상위 준위와 하위 준위의 물리적인 전송 대역, 버퍼 용량, 네트워크 기반 서비스 거부 공격에 소모된 자원, 허용 가능한 공격 소스 수 및 손실 확률에 대한 관계를 분석한 제한 조건을 도출한 후 이에 대한 네트워크 노드의 자원과 비용의 관계를 분석하여 보장된 가용성을 유지할 수 있는 경제적 노드의 자원 구성을 설계하고자 하였다.

먼저, 비정상 공격 세션 트래픽의 통계적 특성에 따른 손실 없는 서비스를 위한 유효대역폭을 산출하였다. 이를 바탕으로 할당된 대역폭에 대하여 손실 없는 서비스를 보장할 수 있는 최대 공격 세션 수와 공격 소스 수에 따른 손실 확률을 도출하여 서비스의 품질 정도를 분석하였으며 목적된 서비스 품질(손실 확률)을 보장하는 대역폭을 산출하였다.

마지막으로 서비스 가용성 유지를 위한 손실 확률과 노드 구축 비용과의 상관관계를 분석하여 예산된 구축 비용에 대하여 수용 가능한 서비스 품질을 예상할 수 있으며 또한, 목적된 서비스 품질을 보장함과 동시에 자원 낭비를 제거하여 망 구성 비용을 최적화 할 수 있는 네트워크 구성 방법을 예시하였다.

따라서 본 연구 결과는 네트워크 서비스 공격에 대응하기 위해, 허용된 서비스 거부 확률에 기반을 둔 보장된 서비스를 유지할 수 있는 효율적인 보안 네트워크 구조 설계에 기여할 것으로 기대되며 물리적인 네트워크 구성 요소에 의한 예방책이 아닌

논리적인 요소에 의해 서비스 거부 공격에 감내하여 목적된 손실 확률을 보장할 수 있는 네트워크 프로토콜 분석에 의한 연구도 현재 진행 중에 있다.

참 고 문 헌

[1] A. Elwalid and D. Mitra, "Effective bandwidth of general markovian traffic sources and admission control of high speed networks," *IEEE TRANS on Networking.*, Vol. 1, no. 3, pp.329 - 341, June, 1993.

[2] B. T. Doshi, "Deterministic rule based traffic descriptors for broadband ISDN: worst case behavior and connection acceptance control," *Proc. IEEE GLOBECOM '93*, pp.1759-1764, Nov, 1993.

[3] A. Elwalid, D. Mitra, and R. Wentworth, " A new approach for allocating buffers and bandwidth to heterogeneous, regulated traffic in an ATM node," *IEEE J. on Select Area in Commun*, Vol. 13, no. 6, pp.1115-1127, Aug, 1995.

[4] G.Ramamurthy and Q. Ren, "Multi-class connection admission control policy for high speed ATM switches," *Proc. IEEE INFOCOM '97*, pp.965-974, Mar, 1997.

[5] L. Kosten, "Liquid models for a type of information storage problems," *Delft Prog. Rep.: Math. and Inform.* Eng., Vol. 11, pp.71-86, 1986.

[6] R. Guerin, H, Ahmadi, and M. Nagshineh, "Equivalent capacity and its application to bandwidth allocation in high-speed networks," *IEEE J. on Select Area in Commun*, Vol. 9, No.7, pp.968-981, Sep 1991.

[7] S. A. Barnett and G. J. Anido, "A cost comparison of distributed and centralized approaches to Video-on-Demand," *IEEE J. Select. Areas In Commu.*, vol. 14, no. 6, pp1173 - 1183, Aug, 1996.

[8] "서비스 거부 공격과 대책, " avilable via at http://www.certcc.or.kr/advisory/tr/DOS-1.html.

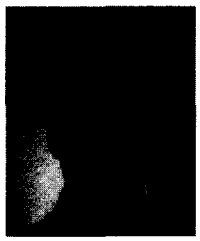
[9] 이현우, 정현철, "분산 환경에서의 서비스거부 공격 분석 보고서," available via at http://certcc.or.kr/paper/tr1999/1999010/tr1999010.html.

[10] Steve Gibson, "The Distributed Reflection DoS Attack," available via at http://grc.com/dos/drdos.htm.

백 남 균(Nam-Kyun Baik) 정회원

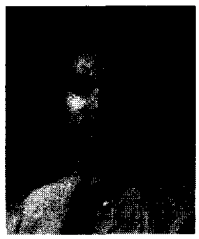
1998년 2월 : 숭실대학교 전자공학과 졸업
1998년~1999년 : IntSecu Corp 연구개발부
2001년 2월 : 숭실대학교 전자공학과 석사
2000년~현재 : 한국정보보호진흥원 산업지원단 평가2팀
<관심분야> 네트워크 보안, 네트워크 QoS, 정보통신시스템 감사

김 지 훈(Ji-Hoon Kim) 정회원



1999년 8월 : 중앙대학교 컴퓨터공학과 졸업
2003년 8월 : 아주대학교 정보통신공학과 석사
1999년~현재 : 한국정보보호진흥원 산업지원단 평가2팀
<관심분야> 네트워크 보안, 무선보안

신 화 종(Hwa-Jong Shin) 정회원



1999년 2월 : 세종대학교 전산과학과 졸업
2001년 2월 : 세종대학교 전산학과 이학석사
2001년~현재 : 한국정보보호진흥원 산업지원단 평가2팀
<관심분야> 네트워크 보안, 소프트웨어 공학, 무선통신보안

이 완 석(Wan-Suck Yi) 정회원

1991년 5월 : Va. Tech 전산과학과 졸업
1994년~1996년 : 현대정보기술 CAD/CAM 사업부
2001년 2월 : 동국대학교 정보보호학과 석사
1996년~현재 : 한국정보보호진흥원 산업지원단 평가2팀장
<관심분야> 모빌코드 보안, 스마트카드 보안, 정보전, 네트워크 보안, PKI