논문 2006-43TC-7-9

# 공격차단 기법과 공격경감 기법 간 이론적 성능 분석

## ( Theoretical Performance Analysis between Attack Prevention Schemes and Attack Mitigation Schemes )

고 광 선*, 엄 영 익**

( Kwangsun Ko and Young Ik Eom )

요 약

서비스거부 공격 또는 분산서비스거부 공격과 같이 단시간 동안 대량의 비정상 트래픽이 발생하였을 경우, 이에 대응하기 위한 기법들에 대해 많은 연구가 진행되었다. 본 논문에서는 비정상 트래픽에 대응하기 위한 대표적인 기법들인 공격차단 기법과 공격경감 기법을 이론적으로 비교한 내용을 보이고자 한다. 공격차단 기법은 일반적으로 필터링 규칙을 기반으로 특정 네트워크로 유입된 네트워크 트래픽에 대해 통과 또는 차단을 실시하는 기법을 의미한다. 그리고 공격경감 기법은 트래픽 전송경로 상에 존재하는 라우터에서 각 라우터들이 가지고 있는 비정상 트래픽 정보를 기반으로 해당 트래픽에 대해 필터링 작업을 실시하거나, 목적지 네트워크의 게이트웨이 상에서 유입된 트래픽의 서비스품질을 제어하는 방법으로 비정상 트래픽에 대해 대응 작업을 실시하는 기법을 의미한다. 비교 기준으로는 공격탐지루틴이 동작한 후, 통과하는 정상 트래픽과 오탐지 트래픽 비율로 하며, 공격경감 기법에 사용할 수 있는 구체적인 트래픽 대역폭 비율을 추가로 보이도록 한다.

Abstract

To defeat abnormal traffic driven by DoS (Denial-of-Service) or DDoS (Distributed DoS), there has been a variety of researches or studies in a few decades. In this paper, we present the results of theoretical performance analysis between attack prevention schemes and attack mitigation schemes. The former is a scheme that prevents abnormal incoming traffic from forwarding into a specific network based on filtering rules, and the latter is a scheme that makes some perimeter or intermediate routers, which exist on the traffic forwarding path, prevent abnormal traffic based on their own abnormal traffic information, or that mitigates abnormal traffic by using quality-of-service mechanisms at the gateway of the target network. The aspects of theoretical performance analysis are defined as the transit rates of either normal traffic or false-positive traffic after an attack detection routine processes its job, and we also present the concrete network bandwidth rates to control incoming traffic.

**Keywords :** attack prevention, attack mitigation, theoretical performance analysis, abnormal traffic

## I. 서 론

분산서비스거부 공격은 단시간에 대량의 비정상 트래픽을 발생시켜 공격대상 시스템 또는 네트워크 자원을 무력화시키는 특성을 가지고 있다. 그러나 1988년 모리스 웜이 등장한 이후, 최근에는 Nimda, Code Red, 그리고 Slammer와 같은 웜에 의해 발생한 비정상 트래픽이 분산서비스거부 공격과 유사한 양상으로 특정 자원에 대한 공격을 실시하고 있으며, 해결해야 하는 중요한 사회적 문제로 등장하고 있다[1][2][3][4][5]. 이에 대한 대표적인 사례로는 2003년 1월 25일 발생한 인터넷대란을 들 수 있다.

이러한 비정상 트래픽을 차단하기 위하여 진행되고 있는 연구를 구분하면 크게 공격차단 기법과 공격경감 기법으로 구분할 수 있다. 공격차단 기법은 오용탐지 또는 비정상행위탐지 메커니즘을 기반으로 공격 트래픽을 차단하고, 정상 트래픽을 통과시키는 기법으로, 주로 특정 네트워크의 게이트웨이 시스템에 적용된다. 이러한 기법은 현재 가장 많이 연구되고 있는 분야이면서

* 학생회원, ** 정회원, 성균관대학교 정보통신공학부
(School of Info. and Comm. Eng., Sungkyunkwan University)
※ 본 연구는 정보통신부 대학 IT연구센터 육성·지원 사업의 연구결과로 수행되었습니다.
접수일자: 2006년6월15일, 수정완료일: 2006년7월14일

제품화할 수 있는 가장 확실한 기법으로 인식되고 있지만, 공격탐지루틴의 탐지 성능에 따라 해당 시스템의 성능이 결정되며, 비정상 트래픽을 탐지하지 못하는 미탐지(false-negative) 가능성과 정상 트래픽을 비정상 트래픽으로 탐지하여 차단하는 오탐지(false-positive) 가능성이 존재한다.

공격경감 기법의 경우에는 학계와 연구소에서 주로 연구되고 있으며, 다시 두 가지 기술로 세분화할 수 있다. 첫 번째는 공격 트래픽의 출발지와 도착지의 전송 경로에 존재하는 라우터들이 해당 트래픽을 단계적으로 필터링을 함으로써 공격파장을 상쇄시키는 라우터기반 공격경감 기법[6][7][8][9]이고, 두 번째는 최종 목적지 네트워크의 게이트웨이 위치에서 네트워크 대역폭을 제한함으로써 해당 공격을 경감시키는 게이트웨이기반 공격경감 기법[10][11][12]이다. 즉, 라우터기반 공격경감 기법은 다수의 라우터에서 가지고 있는 비정상 트래픽 정보를 기반으로 필터링을 실시하여 거시적인 관점에서 비정상 트래픽을 경감시키는 기법이라면, 게이트웨이기반 공격경감 기법은 서비스품질제어 메커니즘을 이용하여 미시적인 관점에서 비정상 트래픽을 경감시키는 기법이다.

전자의 경우, 주로 IP Traceback 메커니즘을 이용하여 공격판단 결과를 중간 라우터에게 전달함으로써 중간 라우터가 해당 공격을 상쇄시키도록 한다. 그러나 IP Traceback 기법을 사용할 경우 모든 중간 라우터로의 정보전달의 한계가 존재할 수밖에 없으며, 정보전달을 위한 프로토콜을 정의하기 어렵다는 단점이 있다. 후자의 경우에는 가장 현실적인 공격경감 기법이지만, 대역폭을 제한하는 구체적인 알고리즘과 이와 관련된 설정 값을 결정하기 어렵다.

본 논문에서는 게이트웨이기반 공격경감 기법의 성능을 분석하기 위하여 공격차단 기법과 비교 및 분석한 결과를 설명한다. 구체적으로 정상 트래픽, 비정상 트래픽, 그리고 오탐지 트래픽 관점에서 비교 및 분석하며, 네트워크 대역폭을 제한하기 위한 구체적인 네트워크 대역폭 비율을 제시한다. 따라서 본 논문에서는 특정 네트워크로 유입된 트래픽의 비정상 유무를 탐지하는 새로운 접근 방법을 제시하는 것이 아니라, 공격탐지루틴이 동작하여 분류된 트래픽을 어떻게 처리하는 것이 정상 트래픽을 최대한 보장해 줄 수 있고, 오탐지 트래픽을 최소화 할 수 있는지에 대한 기준을 제시한다. 게이트웨이기반 공격경감 기법(이하 공격경감 기법이라 칭함)을 구체적 어떻게 구현할 수 있는지에 대한 설명은 관련 논문[13][14]에 자세히 설명되어 있다.

본 논문의 구성은 다음과 같다. II장에서는 공격차단 기법과 서비스품질제어 메커니즘을 이용한 네트워크 대역폭을 조절하는 공격경감 기법 간 비교를 위해 필요한 전제조건과 트래픽을 분류한 내용에 대해 설명하며, III장에서는 공격차단 기법과 공격경감 기법 간 비교 및 분석 결과를 보인다. IV장에서는 공격경감 기법과 관련한 기존 연구 내용을 보이고, 마지막 V장에서는 결론을 제시한다.

## II. 전제조건 및 정의

본 장에서는 공격차단 기법과 공격경감 기법 간 비교 및 분석을 위해 요구되는 전제조건을 보이고, 트래픽의 종류를 정의한다.

### 1. 전제조건

네트워크 트래픽은 일반적으로 연속된 시간상의 패킷 흐름으로 정의할 수 있으나, 본 논문에서는 비교 및 분석의 용이함을 위하여 이산 시간상에 존재하는 패킷 흐름으로 정의한다. 따라서 임의의 시각 $i$에는 패킷의 출발지 주소와 도착지 주소를 쌍으로 하는 다수의 서브 트래픽이 존재할 수 있으며, 정상 트래픽 $N_i$을 $\sum_{k=1}^{n} N_{i,k}$로 정의할 수 있다. 그리고 임의의 시각 $i$에 존재하는 비정상 트래픽 $A_i$은 전체 트래픽 $T_i$에서 정상 트래픽 $N_i$을 제외한 나머지 트래픽으로 정의할 수 있다. $A_i$에 대해 이러한 정의가 가능한 이유는 본 논문에서는 미탐지(false-negative) 트래픽은 고려하지 않고, 오탐지(false-positive) 트래픽만 고려하기 때문이다. 즉, 일반적으로 공격탐지루틴의 성능평가 측면(공격 유무 판단 시점)에서 미탐지 트래픽은 매우 중요한 요소이지만, 본 논문에서는 공격탐지루틴이 동작한 후 비정상이라고 판단된 트래픽을 어떻게 처리하는 것이 보다 더 많은 정상 트래픽을 보장해 줄 수 있고, 오탐지되는 비율을 보다 더 낮게 유지할 수 있는지에 대한 측면(판단 후 시점)만을 고려하기 때문이다. 따라서 특정 네트워크로 유입된 트래픽은 공격탐지루틴이 동작하여 정상 트래픽과 비정상 트래픽(오탐지 트래픽 포함)으로 구분되며, $T_i = N_i + A_i$가 성립한다. 오탐지 트래픽은 공격탐지루틴에 의해 정상 트래픽이 비정상 트래픽으로 판단된 트래픽이므로 $A_i$의 일부분에 해당하며, 공격탐지루틴의 성능에 따라 결정되기 때문에, 오탐지 트래픽 $F_i$는

표 1. 용어 정의
Table 1. Definitions.

| | 정 의 | 비 고 |
|---|---|---|
| $N_i$ | $\sum_{k=1}^{n} N_{i,k}$ | $N_{i,k}$: 임의의 시각 $i$에서 $N_i$의 $k$번째 서브트래픽 |
| $A_i$ | $T_i - N_i$ | $T_i$: 전체 트래픽 |
| $F_i$ | $pA_i\ (0 \le p \le 1)$ | $p$: 오탐지율 |
| $i$ | 공격탐지루틴이 동작하는 임의의 시각 | - |

$pA_i(0 \le p \le 1)$으로 정의할 수 있다. 이에 대한 자세한 내용을 표 1에서 보인다.

표 1을 기반으로 임의의 시각 $i$에 특정 네트워크로 유입되는 전체 트래픽, 정상 트래픽, 비정상 트래픽, 그리고 오탐지 트래픽의 관계를 정의하면 식 (1)을 만족한다.

$$T_i = N_i + (1-p)A_i + F_i (0 \le p \le 1) \quad (1)$$

임의의 시각 $i$에 유입된 트래픽의 비정상 유무를 판단한 공격탐지루틴은 $i+1$ 시각에 다시 동작하여 비정상 유무를 판단하면, $i$ 시각부터 $i+1$ 시각까지의 시간을 $\tau$로 정의할 수 있다. 따라서 공격탐지루틴은 슬라이딩 타임윈도우를 $\tau$로 하여, $\tau$ 동안 유입된 트래픽의 비정상 유무를 결정한다. 공격탐지루틴은 이미 많은 연구가 진행된 오용탐지 메커니즘 또는 비정상행위탐지 메커니즘으로 구성할 수 있으며, 본 논문에서는 구체적인 공격탐지 메커니즘과 $\tau$의 값은 논의하지 않는다.

공격차단 기법과 공격경감 기법을 비교하기 위해서 기준이 되는 항목으로는 동일한 공격탐지루틴이 입력 트래픽에 대한 분류작업을 실시하였을 때, 분류회수에 상관없이 임의의 시각에 통과하는 정상 트래픽의 비율과 오탐지 트래픽의 비율인 $\rho$와 $\theta$로 정의한다.

## 2. 트래픽 분류

표 1에서 정의한 내용을 기준으로, 공격탐지루틴이 $\tau$ 동안 특정 네트워크로 유입된 트래픽에 대하여 임의의 시각 $i$에 비정상 유무를 판단하였을 경우, 정상 트래픽과 비정상 트래픽이 각각 $\alpha$($T_i$에서 $N_i$이라고 판단한 비율)와 $\beta$($T_i$에서 $A_i$라고 판단한 비율)만큼 존재한다고 가정하자. 따라서 $\tau$ 동안 유입된 트래픽 $T_i$에는 정상 트래픽, 비정상 트래픽, 그리고 오탐지 트래픽이 각각 $N_i = \alpha T_i$, $A_i = (1-p)\beta T_i$, 그리고 $F_i = p\beta T_i$ 만큼 존재하며, $\alpha$와 $\beta$는 공격탐지루틴에 종속적이기 때문에

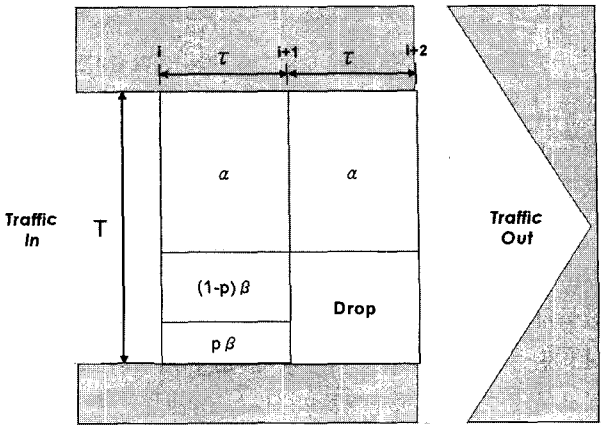


그림 1. 공격차단 기법을 적용하였을 경우 각 트래픽별 비율
Fig. 1. The rates of each traffic in case of adopting an attack prevention scheme.

시간에 관계없는 상수로 존재한다.

공격차단 기법은 일반적으로 $\tau$ 마다 공격탐지루틴이 동작하여 트래픽 필터링 규칙을 생성(관리자에 의한 수동 생성 또는 공격탐지루틴에 의한 자동 생성)한 후, 유입된 트래픽을 차단하거나 통과시킨다. 즉, $i$ 시각부터 $i+1$ 시각까지 유입된 트래픽이 공격탐지루틴에 의해 정상 트래픽, 비정상 트래픽, 그리고 오탐지 트래픽이 이러한 기법은 필터링 규칙의 정확성 유무와는 상관없이 각각 $\alpha$, $(1-p)\beta$, 그리고 $p\beta$ 비율로 분류되고, $i+1$ 시각에 정상 트래픽은 통과하지만, 비정상 트래픽과 오탐지 트래픽은 차단된다. 이에 대한 구체적인 내용은 그림 1과 같다.

그림 1에서 보이는 바와 같이, 트래픽이 유입되어 공격차단 기법이 적용된 보안시스템의 좌측에서 우측 방향으로 통과할 때, 임의의 시각 $i$부터 $i+1$ 시각까지 $\tau$ 동안 유입된 트래픽은 공격탐지루틴에 의해 정상 트래픽과 비정상 트래픽이 각각 $\alpha$와 $\beta$의 비율만큼 구분되고, 오탐지 트래픽은 $p\beta$ 비율만큼 구분된다. 이러한 결과를 기반으로 $i+1$ 시각부터에 유입되는 트래픽에 대응하기 위하여 필터링 규칙을 생성되며, 생성된 필터링 규칙은 $i+1$ 시각에 비정상 트래픽이라고 판단한 $\beta$ 비율만큼의 트래픽을 차단하고, 정상 트래픽이라고 판단한 $\alpha$ 비율만큼의 트래픽을 통과한다. 오탐지 트래픽은 $p\beta$ 비율만큼 존재하며, 공격탐지루틴에서 비정상 트래픽으로 판단되기 때문에 차단된다.

공격차단 기법이 적용된 보안 시스템이 이러한 방식으로 동작하기 위해서는 $i$ 시각부터 $i+1$ 시각까지 $\tau$ 동안 유입된 트래픽에 대해 공격탐지루틴이 비정상 유무를 판단하고, 이 결과를 다음 시각 $i+1$에 적용할 수

있도록 신속하게 동작하는 시스템이 구성되어야 한다. 그러나 이러한 부분은 구현 측면에서의 고려사항이기 때문에 본 논문에서는 추가적으로 언급하지 않도록 한다. 또한 $i+1$ 시각에 차단 대상이 되는 트래픽은 $i$ 시각부터 $i+1$ 시각까지 유입된 트래픽이며, $i+1$ 시각부터 $i+2$ 시각까지 $\tau$ 동안 새로이 트래픽이 유입되어 $\alpha$와 $\beta$의 비율이 달라질 수 있다. 그러나 공격차단 기법이 적용된 보안시스템이 대응하고자 하는 공격은 대규모의 비정상 트래픽이 한정된 네트워크 대역폭을 단시간 동안 통과하는 양상을 보이기 때문에 그림 1과 같이 동작하는 $\tau$ 동안 새로운 연결 요청이나 새로운 세션이 발생할 가능성이 낮기 때문이다.

공격경감 기법은 공격차단 기법과 동일한 공격탐지루틴을 사용하지만, 트래픽 필터링 규칙 대신 트래픽의 서비스품질제어 규칙을 생성(관리자에 의한 수동 생성 또는 공격탐지루틴에 의한 자동 생성)하여 유입된 트래픽에 적용한다. 이러한 기법은 비정상 트래픽으로 정확히 판단되기 전까지 의심 트래픽으로 처리하도록 구성되기 때문에, 전체 트래픽은 최초 $\tau$ 시간 후에는 정상 트래픽과 의심 트래픽으로 구분되고, 두 번째 $\tau$ 시간 후에는 정상 트래픽, 비정상 트래픽으로 구분된다(단, 두 단계로 공격을 경감할 경우에 한함). 즉, 공격탐지루틴이 첫 번째로 판단한 결과 중 비정상 트래픽은 의심 트래픽으로 처리하고, 이 의심 트래픽을 다음 $\tau$ 동안에 재판단하여 정상 트래픽과 비정상 트래픽으로 다시 구분한 후, 비정상 트래픽만을 차단함으로써, 통과하는 정상 트래픽의 비율을 높일 수 있고, 오탐지 트래픽의 비율을 낮출 수 있다. $\tau$ 시간마다 구분되는 정상 트래픽, 비정상 트래픽, 그리고 오탐지 트래픽의 비율은 그림 2와 같다.

그림 2에서 보이는 바와 같이, 임의의 시각 $i$부터 $i+1$ 시각까지 $\tau$ 동안 유입된 트래픽은 공격탐지루틴에 의해 정상 트래픽과 의심 트래픽으로 판단되며, $i+1$ 시각에 정상 트래픽은 $\alpha$ 비율만큼, 의심 트래픽은 $\beta$ 비율만큼 통과하도록 서비스품질을 조절한다. 마찬가지로, 오탐지 트래픽은 $p\beta$ 비율만큼 통과하도록 서비스품질을 조절한다. 이렇게 서비스품질이 조절된 트래픽들은 $i+1$ 시각부터 $i+2$ 시각까지 $\tau$ 동안 공격탐지루틴에 의해 재분류된다. 즉, $\alpha$만큼은 정상 트래픽으로 계속 통과시키지만, $\beta$만큼의 의심 트래픽에 대해서는 $\alpha\beta$ 비율만큼은 정상 트래픽으로, $(1-p)\beta^2$ 비율만큼은 비정상 트래픽으로, 그리고 $p\beta^2$ 비율만큼은 오탐지 트래픽으로 판단된다. 따라서 $i+2$ 시각에는 $\alpha+\alpha\beta$ 비율만큼의 정상 트래픽만 통과하게 되고, 나머지 트래픽들은 차단된다.

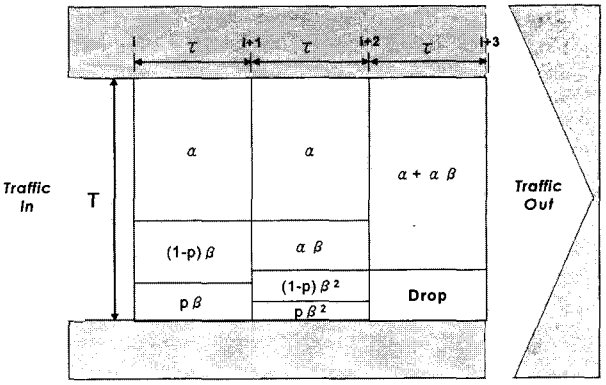


그림 2. 공격경감 기법을 적용하였을 경우 각 트래픽별 비율

Fig. 2. The rates of each traffic in case of adopting an attack mitigation scheme.

공격경감 기법이 적용된 보안 시스템이 이러한 방식으로 동작하기 위해서는 몇 가지 고려사항이 요구된다. 첫째로 본 논문에서 설명하는 공격경감 기법은 두 단계 경감을 실시한다. 그림 2에서 보이는 바와 같이 최초 단계에서는 유입된 트래픽을 정상 트래픽과 의심 트래픽을 구분하고, 그 다음 단계에서는 의심 트래픽을 정상 트래픽, 비정상 트래픽, 그리고 오탐지 트래픽으로 구분하는 방식으로 동작한다. 만일 세 단계 경감을 실시한다면, 최초에 정상 트래픽과 의심 트래픽으로 구분하고, 그 다음에는 의심 트래픽을 정상 트래픽과 의심 트래픽으로 구분하며, 마지막에 의심 트래픽을 정상 트래픽과 비정상 트래픽으로 동작하는 것을 의미한다. 두 번째로는 기 설명한 바와 같이 $i$ 시각부터 $i+1$ 시각까지 $\tau$ 동안 유입된 트래픽에 대해 공격탐지루틴이 비정상 유무를 판단하고, 이 결과를 다음 시각 $i+1$에 적용할 수 있도록 신속하게 동작하는 시스템이 구성되어야 한다. 세 번째로는 $i+1$ 시각에 차단 대상이 되는 트래픽은 $i$ 시각부터 $i+1$ 시각까지 유입된 트래픽이며, $i+2$ 시각에 차단 대상이 되는 트래픽은 $i$ 시각부터 $i+2$ 시각까지 $2\tau$ 동안 계속해서 유입되는 동일한 출발지와 도착지 주소를 가지는 트래픽이다. 즉, 새로이 유입된 트래픽이 존재하지 않는다고 가정한다. 이러한 가정이 가능한 이유는 다음과 같다. 공격경감 기법이 적용된 보안시스템이 대응하고자 하는 공격은 대규모의 비정상 트래픽이 한정된 네트워크 대역폭을 단시간 동안 통과하는 양상을 보이기 때문에 그림 2와 같이 동작하는 $2\tau$ 동안 새로운 연결 요청이나 새로운 세션이 발생할 가능성이 낮기 때문이다.

## Ⅲ. 공격차단 기법과 공격경감 기법 간 분석

본 장에서는 공격차단 기법과 공격경감 기법 간 비교 및 분석을 위하여 동일한 공격탐지루틴이 동작한 후에 보안 시스템을 통과하는 정상 트래픽 비율과 오탐지 트래픽 비율을 확인하고, 공격경감 기법에 적용할 수 있는 트래픽 비율을 구체적으로 보이도록 한다.

### 1. 정상 트래픽 비율

본 절에서는 그림 1과 2에서 보이는 내용을 기반으로 공격차단 기법과 공격경감 기법을 정상 트래픽 비율과 오탐지 트래픽 비율 측면에서 비교한 내용을 보인다.

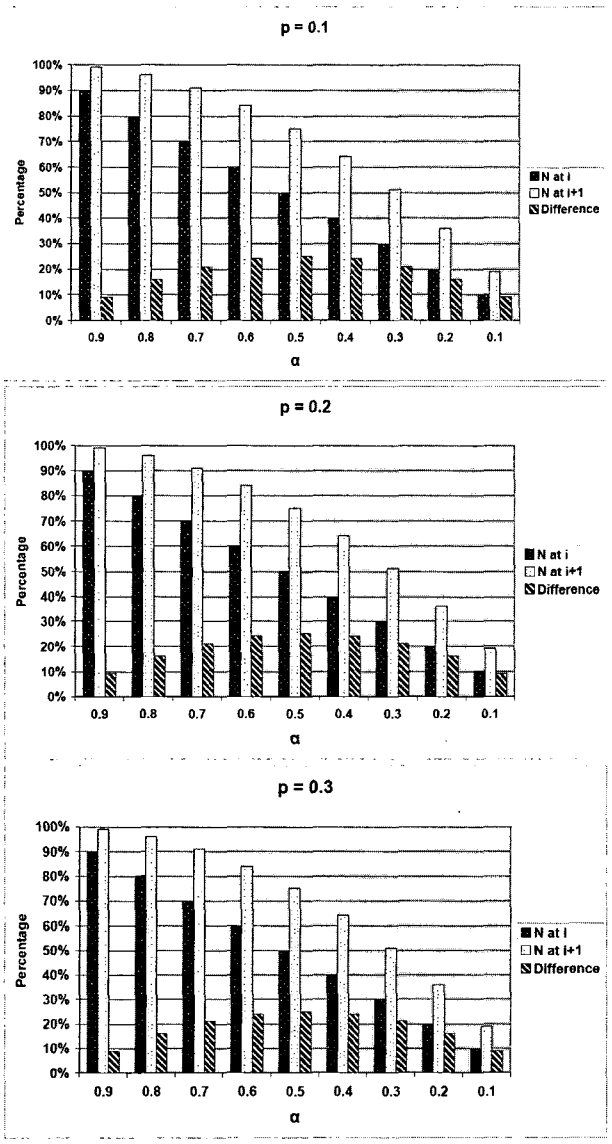


그림 3. 정상 트래픽 비율 측면에서 공격차단 기법과 공격경감 기법 비교

Fig. 3. The results of theoretical comparison between an attack prevention scheme and an attack mitigation scheme in the aspect of normal traffic rate.

먼저 공격차단 기법과 공격경감 기법을 정상 트래픽 비율 측면에서 비교하면 다음과 같다. 전자의 경우, 임의의 시각 $i+1$에 통과하는 $N_i$의 비율은 $\alpha$이므로 정상 트래픽 비율 $\rho$는 수식 (2)와 같다.

$$\rho = \frac{N_i}{T_i} = \alpha \tag{2}$$

공격경감 기법의 경우, 임의의 시각 $i+1$과 $i+2$에 통과하는 평균 정상 트래픽 비율 $\rho$는 수식 (3)과 같다.

$$\rho = \frac{1}{2}\left(\frac{N_i}{T_i} + \frac{N_{i+1}}{T_{i+1}}\right) = \frac{1}{2}(\alpha + \alpha + \alpha\beta) \tag{3}$$

수식 (3)를 $\alpha$로 정리하면 정상 트래픽 비율은 $\rho = -\frac{1}{2}(\alpha - \frac{3}{2})^2 + \frac{9}{8}$ $(0 \le \alpha \le 1)$을 만족한다(임의의 시각 $i$에 유입된 전체 트래픽은 $\alpha$와 $\beta$ 비율로 구분되기 때문에 $\alpha + \beta = 1$ 관계를 만족함). 식 (2)와 (3)간에는 $\alpha = 0.5$ $(\frac{d\rho}{d\alpha} = -\alpha + \frac{1}{2})$에서 가장 큰 정상 트래픽 비율 차가 존재하며, 공격경감 기법이 공격차단 기법보다 많은 정상 트래픽을 통과시킨다. 이는 공격경감 기법이 $i+1$ 시각에 $\alpha\beta$비율만큼의 정상 트래픽을 추가로 통과시키기 때문이다. 공격차단 기법이 적용된 $i$ 시각과 공격경감 기법이 적용된 $i+1$ 시각에서 정상 트래픽 비율의 구체적인 내용을 그림 3에서 보인다.

### 2. 오탐지 트래픽 비율

공격차단 기법과 공격경감 기법을 오탐지 트래픽 비율 측면에서 비교하면 다음과 같다. 전자의 경우, 임의의 시각 $i+1$에 통과하는 $F_i$의 비율은 $p\beta$이므로 오탐지 트래픽 비율 $\theta$는 수식 (4)와 같다.

$$\theta = \frac{F_i}{T_i} = p\beta \tag{4}$$

공격경감 기법의 경우, 임의의 시각 $i+1$과 $i+2$에 통과하는 평균 정상 트래픽 비율 $\theta$는 수식 (5)와 같다.

$$\theta = \frac{1}{2}\left(\frac{F_i}{T_i} + \frac{F_{i+1}}{T_{i+1}}\right) = \frac{1}{2}(p\beta + p\beta^2) \tag{5}$$

수식 (5)를 $\alpha$로 정리하면 오탐지 트래픽 비율은 $\theta = \frac{p}{2}(\beta^2 + \beta)$ $(0 \le \beta \le 1)$을 만족한다(임의의 시각 $i$에 유입된 전체 트래픽은 $\alpha$와 $\beta$ 비율로 구분되기 때문

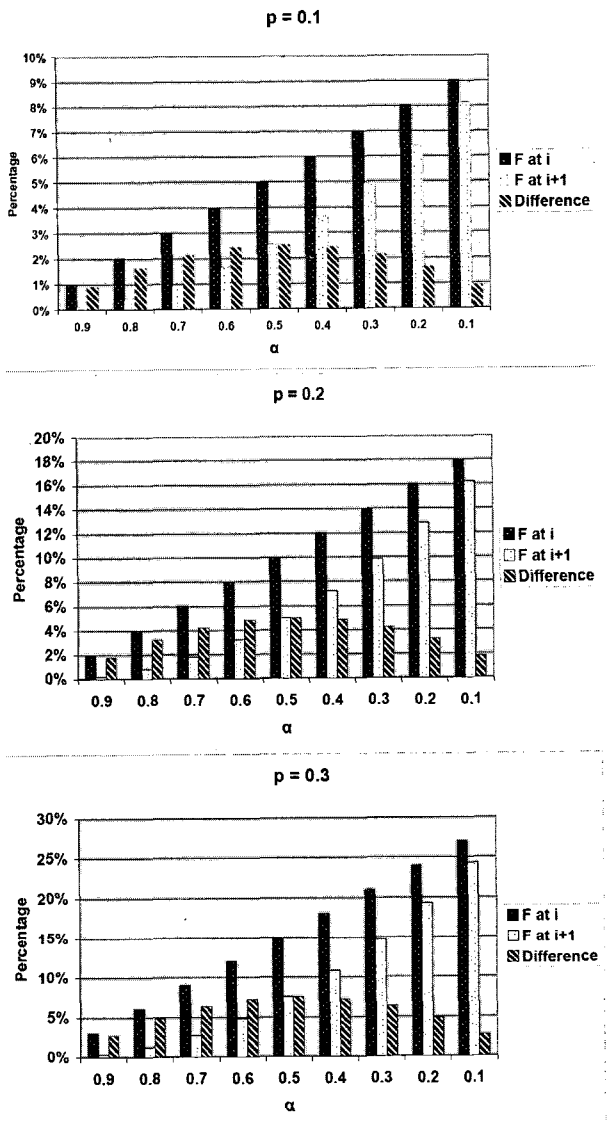


그림 4. 오탐지 트래픽 비율 측면에서 공격차단 기법과 공격경감 기법 비교

Fig. 4. The results of theoretical comparison between an attack prevention scheme and an attack mitigation scheme in the aspect of false-positive traffic rate.

에 $\alpha+\beta=1$ 관계를 만족함). 식 (4)와 식 (5)간에는 $\beta=0.5$ ($\frac{d\theta}{d\beta}=-\beta+\frac{1}{2}$)에서 가장 큰 오탐지 트래픽 비율 차가 존재하며, 공격경감 기법이 공격차단 기법보다 적은 오탐지 트래픽을 통과시킨다. 이는 공격경감 기법이 $i+1$ 시각에 $p\beta^2$비율만큼의 오탐지 트래픽만 통과하기 때문이다. 공격차단 기법이 적용된 $i$ 시각과 공격경감 기법이 적용된 $i+1$ 시각에서 정상 트래픽 비율의 구체적인 내용을 그림 4에서 보인다.

### 3. $\alpha$와 $\beta$ 비율

일반적으로 네트워크 게이트웨이 위치에 설치되는 보안시스템에 적용할 수 있는 공격경감 기법의 경우, 네트워크 대역폭을 조절하여 특정 트래픽의 서비스품질을 제어하게 되므로, 결과적으로 정확히 비정상으로 판단된 트래픽만 차단하고, 의심 트래픽은 낮은 출력 대역폭으로 통과하게 한다. 이러한 공격경감 기법은 비정상 트래픽에 의한 공격 여파를 지연시킬 수 있기 때문에 공격 차단기법에 비하여 오탐지율을 최소화 시킬 수 있으므로, 현실적으로 효과적인 비정상 트래픽 대응 기법으로 생각할 수 있다. 그러나 공격탐지루틴에 의해 판단된 결과로 생성되는 서비스품질제어 규칙을 어떠한 기준으로 생성할 것인가에 대한 문제가 발생한다. 그 기준은 정상 트래픽과 의심 트래픽이 통과하는 대역폭을 얼마로 지정할 것인지에 대한 기준이다. 즉, 정상 트래픽 비율인 $\alpha$를 얼마로 할당하였을 경우에 효과적으로 단시간동안 대량으로 발생하는 비정상 트래픽에 대한 대응이 가능한 지에 대한 문제이다.

본 절에서는 분석의 용이함을 위하여, 특정 네트워크로 유입된 트래픽은 고정 할당된 대역폭을 통과하고, 정상 트래픽이 통과하는 대역폭과 의심 트래픽이 통과하는 대역폭이 정적으로 설정되어 있다고 가정한다. II 장 2절에서 설명한 공격경감 기법의 트래픽 분류 내용을 기반으로 $i+1$ 시각에 정상 트래픽의 비율 ($N_{i+1}$), 비정상 트래픽의 비율 ($A_{i+1}$), 오탐지 트래픽의 비율 ($F_{i+1}$), 그리고 비정상 트래픽과 오탐지 트래픽 합 ($A_{i+1}+F_{i+1}$)의 비율을 확인하면 그림 5와 같다.

그림 5에서 보이는 바와 같이, 비정상 트래픽과 오탐지 트래픽의 합은 $p$에 관계없이 일정함을 알 수 있는데, 이는 표 1과 식 (1)을 통하여 확인할 수 있다. 결국 $p$는 비정상 트래픽과 오탐지 트래픽에만 종속적인 변수이기 때문에 동일한 공격탐지루틴이 실행되고 있는 상황에서는 공격경감 기법에 영향을 미치지 않는다. 정상 트래픽용 네트워크 대역폭을 전체 트래픽의 30% 이상 할당할 경우, 정상 트래픽은 항상 전체 트래픽의 50% 이상을 차지하며 비정상 트래픽보다 높은 비율로 통과한다. 즉, 정상 트래픽이 통과할 수 있도록 정적으로 네트워크 대역폭을 전체 대역폭의 30% 이상으로 할당할 경우, 해당 보안 시스템은 50% 이상의 정상 트래픽이 통과하도록 보장하면서 네트워크를 보호할 수 있으며, 단시간동안 많은 양의 비정상 트래픽이 발생하더라도 최대 50%를 초과하지 않도록 제어할 수 있으므로 공격 대응시간을 충분히 확보할 수 있다.

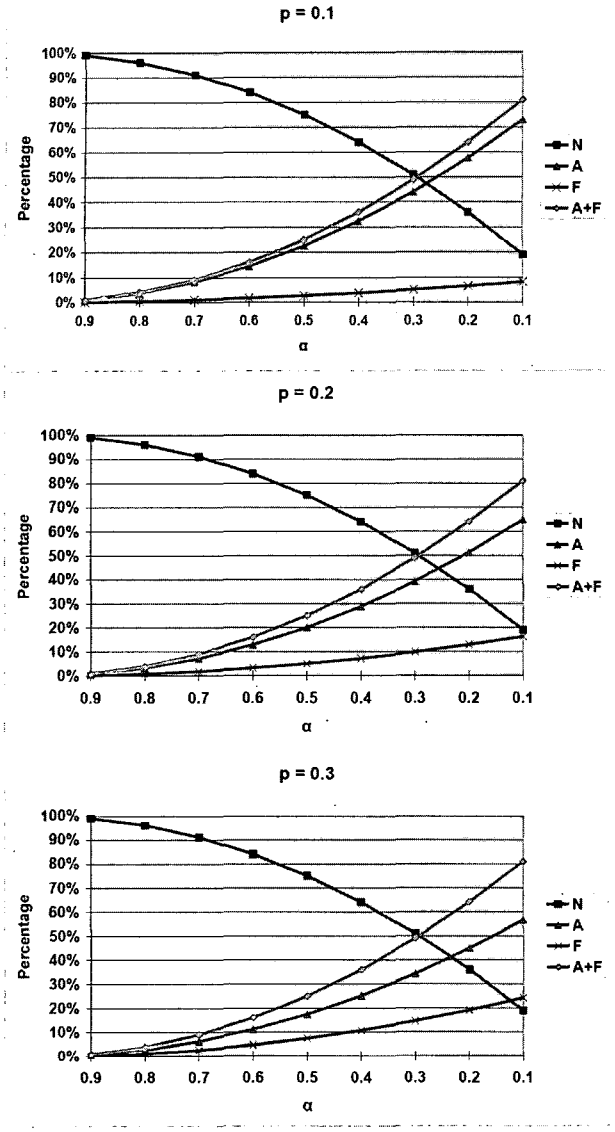


그림 5. $i+1$ 시각에 $\alpha$에 따른 정상 트래픽 ($N_{i+1}$), 비정상 트래픽 ($A_{i+1}$), 오탐지 트래픽 ($F_{i+1}$), 그리고 비정상 트래픽과 오탐지 트래픽 합 ($A_{i+1}+F_{i+1}$)이 차지하는 비율

Fig. 5. The rates of normal traffic, abnormal traffic, false-positive traffic, and the sum (abnormal traffic and false-positive traffic) according to $\alpha$, at time $i+1$.

## Ⅳ. 관련연구

공격경감 기법은 크게 라우터기반 공격경감 기법과 게이트웨이기반 공격경감 기법으로 구분할 수 있다. 라우터기반 공격경감 기법은 공격 트래픽의 출발지와 도착지의 전송경로에 존재하는 라우터들이 해당 트래픽을 단계적으로 필터링을 함으로써 공격파장을 상쇄시키는 방법이다. R. K. C. Chang[6]은 비정상 트래픽을 전송하는 근원지에 위치한 라우터에서부터 최종 공격대상 호스트 전에 위치한 라우터까지 단계적으로 비정상 트래픽에 해당하는 트래픽을 차단함으로써 점진적으로 증대되는 분산서비스거부 공격을 차단할 수 있다는 개념을 제시하였다. V. L. L. Thing, et al.[7]은 트래픽 전송에 사용된 설정정보를 재조정하여 출발지 주소에 대한 인증작업을 수행함으로써, 악의적인 사용자가 전송하는 위장된 트래픽을 차단하고, 랜덤하게 생성된 위장 트래픽에 대해서는 적응적 비율제한 기법을 사용하여 대응할 수 있다고 제시하였다. R. Chen, et al.[8]은 공격대상 시스템 근처에서는 공격을 탐지하고 공격 시스템 근처에서는 공격을 방어하는 AD (Attack Diagnosis) 구조를 제시하였다. M. Sung, et al.[9]은 IP Traceback 기법을 이용하여 네트워크 경로가 공격자의 공격 경로 상에 존재하는지 여부를 확인하여 보호하고자 하는 네트워크의 주변 라우터에서 해당 트래픽을 차단하는 기법을 제시하였다.

게이트웨이기반 공격경감 기법은 최종 목적지 네트워크의 게이트웨이 위치에서 네트워크 대역폭을 제한함으로써 해당 공격을 경감시키는 방법이다. F. Kargl[10]은 분산서비스거부 공격으로부터 웹서버를 보호하기 위하여 공격 가능성이 있는 트래픽이 통과하는 네트워크 대역폭을 점차적으로 낮춤으로써 최종적으로 방화벽에서 해당 트래픽을 차단하는 방식으로 동작하는 기법을 제시하였다. A. Gargl, et al.[11]은 서비스거부 공격의 영향을 경감시키기 위하여 리눅스 시스템을 기반으로 프로토타입을 구성하였으며, 서비스품질보장 기술을 기반으로 특정 공격에 의존적이지 않고 일반적으로 대응할 수 있는 기법을 제시하였다. S. Park, et al.[12]은 서비스거부 공격에 대응하기 위하여 대역폭 제어, 방화벽, 침입탐지시스템, 그리고 트래픽 계량과 같은 보안 기능을 제공하는 하드웨어 기반의 SGS (Security Gateway System)을 개발하였다.

## Ⅴ. 결 론

본 논문에서는 단시간동안 대량의 비정상 트래픽을 전송하는 공격에 대응하기 위해서 일반적으로 가장 많이 사용되고 있는 공격차단 기법에 비하여 서비스품질 제어 메커니즘을 이용한 게이트웨이기반 공격경감 기법이 보다 효과적일 수 있다는 사실을 정상 트래픽 비율과 오탐지 트래픽 비율이라는 측면에서 이론적으로 비

교하였다. 또한 게이트웨이기반 공격경감 기법에서 정상 트래픽이 통과할 수 있도록 전체 트래픽의 30% 이상으로 네트워크 대역폭을 할당하여 입력 트래픽의 서비스품질을 제어할 경우, 전체 트래픽의 50% 이상은 항상 정상 트래픽이 통과할 수 있도록 네트워크 대역폭을 유지할 수 있음을 보였다.

향후에는 이론적으로 비교된 결과를 구체적인 시뮬레이션으로 재분석하고, 서비스품질제어 메커니즘을 이용한 게이트웨이기반 공격경감 기법에 대해 보다 일반적이고 포괄적인 분석을 수행하는 연구가 필요할 것이다.

## 참 고 문 헌


[1] S. Staniford, V. Paxson, and N. Weaver, "How to Own the Internet in Your Spare Time," in Proc. of the 11th USENIX Security Symposium (Security '02), pp. 149-167, San Francisco, USA, August 2002.

[2] R. Russell and A. Machie, Code Red II Worm, Technical Report, Incident Analysis, SecurityFocus, August 2001.

[3] A. Machie, J. Roculan, R. Russell, and M. V. Velzen, Nimda Worm Analysis, Technical Report, Incident Analysis, SecurityFocus, September 2001.

[4] CERT/CC, CERT Advisory CA-2001-26 Nimda Worm, http://www.cert.org/advisories/CA-2001-26.html, September 2001.

[5] D. Song, R. Malan, and R. Stone, A Snapshot of Global Internet Worm Activity, Technical Report, Arbor Networks, November 2001.

[6] R. K. C. Chang, "Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial," *IEEE Communications Magazine*, Vol. 40, No. 10, pp. 42-51, October 2002.

[7] V. L. L. Thing, H. C. J. Lee, and M. Sloman, "Traffic Redirection Attack Protection System (TRAPS)," in Proc. of the 20th IFIP International Information Security Conference, pp. 309-326, Chiba, JAPAN, May 2005.

[8] R. Chen and J. M. Park, "Attack Diagnosis: Throttling Distributed Denial-of-Service Attacks Close to the Attack Sources," in Proc. of 14th International Conference on Computer Communications and Networks (ICCCN 2005), pp. 275-280, California USA, October 2005.

[9] M. Sung and J. Xu, "IP Traceback-Based Intelligent Packet Filtering: A Novel Technique for Defending against Internet DDoS Attacks," *IEEE Trans. on Parallel and Distributed Systems*, Vol. 14, No. 9, pp. 861-872, September 2003.

[10] F. Kargl, J. Maier, and M. Weber, "Protecting Web Servers from Distributed Denial of Service Attacks," in Proc. of the 10th International conference on World Wide Web, pp. 514-524, Hong Kong, May 2001.

[11] A. Garg and A. L. N. Reddy, "Mitigation of DoS attacks through QoS regulation," in Proc. of the 10th IEEE International Workshop on Quality of Service (IWQoS2002), pp. 45-53, Miami Beach, USA, 2002.

[12] S. Park, J. Oh, and J. Jang, "High-Speed Attack Mitigation Engine by Packet Filtering and Rate-limiting using FPGA," in Proc. of the 8th International Conference on Advanced Communication Technology (ICACT 2006), pp. 680-685, Gangwon-Do, Republic of Korea, February 2006.

[13] 조은경, 고광선, 이태근, 강용혁, 엄영익, "리눅스 Netfilter 프레임웍과 CBQ 라우팅 기능을 이용한 비정상 트래픽 제어 시스템 설계," *한국정보보호학회논문지*, 한국정보보호학회, Vol. 13, No. 6, pp. 129-140, December 2003.

[14] 고광선, 강용혁, 엄영익, "단계적 비정상 트래픽 대응 기법 설계 및 이론적 분석," *한국정보보호학회 논문지*, 한국정보보호학회, Vol. 16, No. 1, pp. 55-63, February 2006.

## 저 자 소 개


**고 광 선**(학생회원)
1998년 성균관대학교 정보공학과 학사 졸업.
2004년 성균관대학교 전기전자 및 컴퓨터공학부 석사 졸업.
2004년~현재 성균관대학교 정보통신공학부 컴퓨터공학 전공 박사과정.
<주관심분야 : 정보보호, 리눅스, 네트워크>

**엄 영 익**(정회원)
1983년 서울대학교 계산통계학과 학사 졸업.
1985년 서울대학교 전산과학과 석사 졸업.
1991년 서울대학교 전산과학과 박사 졸업.
2000년 9월~2001년 8월: Dept. of Info. and Comm. Science at UCI 방문교수
1993년~현재 성균관대학교 정보통신공학부 교수
<주관심분야 : 분산 컴퓨팅, 이동 컴퓨팅, 이동 에이전트, 시스템 보안, 운영체제, 내장형 시스템>