情報保護學會論文誌
第16卷 第1號, 2006. 2

단계적 비정상 트래픽 대응 기법 설계 및 이론적 분석*

고 광 선,[1†] 강 용 혁,[2] 엄 영 익[1‡]
[1]성균관대학교, [2]극동대학교

Design and Theoretical Analysis of a Stepwise Intrusion Prevention Scheme*

Kwangsun Ko,[1†] Yong-hyeog Kang,[2] Young Ik Eom[1‡]
[1]Sungkyunkwan University, [2]Far East University

요 약

Nimda, Code Red, 그리고 SQL Slammer 등과 같은 웜에 의한 피해 사례가 증가하면서 이를 방어하기 위한 대응 기술 연구가 활발히 진행되고 있다. 본 논문에서는 웜에 의해 발생한 비정상 트래픽을 효과적으로 차단할 수 있는 네트워크 대역폭 조절 방식의 단계적 대응 시스템 설계 내용을 보이고, 기존 패턴 기반 비정상행위탐지 방식의 이원적(True/False) 대응 기법과 이론적으로 비교하고자 한다. 일정 시간동안 특정 네트워크를 통과하는 정상 트래픽 비율과 오탐지 트래픽 비율을 비교 기준으로 하여 두 기법을 이론적으로 비교한 결과, 임의의 시간 동안 전체 네트워크 트래픽에서 비정상 트래픽이 차지하는 비율을 β라고 할 경우, 이원적 대응 기법에 비하여 단계적 대응 기법의 평균 정상 트래픽 비율은 $(1+\beta)/2$만큼 증가하고, 평균 오탐지 트래픽 비율은 $(1+\beta)/2$만큼 감소함을 알 수 있었다.

ABSTRACT

Recently, there is much abnormal traffic driven by several worms, such as Nimda, Code Red, SQL Slammer, and so on, making badly severe damage to networks. Meanwhile, diverse prevention schemes for defeating abnormal traffic have been studied in the academic and commercial worlds. In this paper, we present the structure of a stepwise intrusion prevention system that is designed with the feature of putting limitation, on the network bandwidth of each network traffic and dropping abnormal traffic, and then compare the proposed scheme with a pre-existing scheme, which is a True/False based an anomaly prevention scheme for several worm-patterns. There are two criteria for comparison of the schemes, which are Normal Traffic Rate (NTR) and False Positive Rate (FPR). Assuming that the abnormal traffic rate of a specific network is β during a predefined time window, it is known that the average NTR of our stepwise intrusion prevention scheme increases by the factor of $(1+\beta)/2$ than that of True/False based anomaly prevention scheme and the average FPR of our scheme decrease by the factor of $(1+\beta)/2$.

Keywords : *stepwise Intrusion Prevention Scheme, theorretical analysis*

Ⅰ. 서 론

지난 1.25 인터넷 대란에서 보여주듯이 웜에 의한 공격이 성공하였을 경우, 대규모의 트래픽이 단시간 동안 발생하기 때문에 공격 대상 네트워크는 순식간에 비정상적인 상태에 도달하게 된다[1]. 이러한 웜은 1988년 Morris 웜이 처음 등장한 이후, 지금까지 Code Red, Nimda, 그리고 SQL Slammer 등과 같은 수많은 웜이 지속적으로 등장하고 있으며, 사회 경제적으로 많은 피해를 주고 있다[2-5].

접수일 : 2005년 9월 27일 ; 채택일 : 2006년 1월 2일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 육성지원 사업의 결과로 수행되었음
† 주저자 : rilla91@ece.skku.ac.kr
‡ 교신저자 : yieom@ece.skku.ac.kr

본 논문에서는 웜에 의해서 단시간동안 발생한 대량의 비정상 트래픽을 차단하기 위하여, 패턴 기반 비정상행위탐지 방식의 이원적 (True/False) 대응 기법 (이하 이원적 대응 기법)과 해당 트래픽의 네트워크 대역폭을 조절하는 방식의 단계적 대응 기법을 이론적으로 비교하고자 한다. 비교 기준은 네트워크를 통과하는 정상 트래픽 비율과 오탐지 트래픽 비율로 하며, 본 논문에서 오탐지 트래픽 비율은 False-Positive Rate (FPR)만으로 제한한다. 따라서 본 논문에서는 비정상 트래픽 탐지를 위해 사용되는 비정상 트래픽 탐지 루틴의 알고리즘과 이의 효율성에 대해서는 언급하지 않는다.

본 논문에서 이원적 대응 기법과 단계적 대응 기법 간 이론적 비교를 실시한 이유는 다음과 같다.

- 웜에 효과적인 대응 기법은 어떠한 방식으로 동작해야 하는가? : 최초 웜 발생 후 짧은 시간동안에 많은 호스트들을 감염시키는 웜에 대응하기 위해서는 정상 행위에 해당하는 패턴을 기반으로 한 비정상행위탐지 방식의 이원적 대응 기법이 일반적으로 사용된다. 이 경우 공격 여부를 판단하기 위해서 사용하는 정상 행위에 대한 패턴은 통계적 방식, 인공지능 방식 등과 같이 다양한 방식을 기반으로 만들어질 수 있으며, 네트워크로 유입되는 비정상 트래픽이 패턴과 일치하는지의 여부에 따라서 비정상 여부를 판단한다. 그러나 이러한 방식은 정상 행위 여부를 탐지하는 비정상 트래픽 탐지 루틴의 잘못된 판단으로 인하여 상당한 양의 정상 트래픽이 오탐지되어 차단될 가능성이 존재한다.
- 단계적 대응 기법은 이원적 대응 기법보다 효과적인가? : 정상 행위 여부를 탐지하는 비정상 트래픽 탐지 루틴의 잘못된 판단으로 인하여 차단된 정상 트래픽을 복원시킬 수 있는 단순한 방법으로 비정상 트래픽으로 정확히 판단될 경우에만 해당 트래픽을 차단하도록 하는 기법을 생각할 수 있다. 비정상 트래픽 여부를 확인하기 위하여 특정 네트워크로 유입되는 트래픽에 대해 비정상 트래픽 탐지 루틴을 다수 통과시키도록 함으로써 가장 높은 확률로 비정상 트래픽임을 판단하기 전까지는 모든 트래픽을 '단지 의심되는 비정상 트래픽'으로 판단하는 것이다. 이렇게 함으로써 정상 트래픽이 오탐지되어 비정상 트래픽으로 차단되는 비율을 낮출 수 있다. 본 논문에서는 이러한 방식으로 동작하는 대응 기법을 단계적 대응 기법이라고 정의하고, 이원적 대응 기법과 이론적으로 비교하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 설명하고, 3장에서는 네트워크 대역폭을 조절하는 방식의 단계적 대응 기법에 대하여 설명한 후, 이에 기반한 단계적 대응 시스템 설계 내용을 보인다. 4장에서는 본 논문에서 보여주고자 하는 이원적 대응 기법과 단계적 대응 기법 간 이론적 비교 내용을 보이고, 마지막 5장에서는 결론을 제시한다.

II. 관련 연구

본 장에서는 일반적으로 이원적 대응 기법이 가지는 정상 트래픽의 오탐지 비율을 낮추기 위해 사용되는 대표적인 단계적 대응 기법 두 가지에 대해 간략히 설명하도록 한다. 하나는 인터넷 상에 존재하는 라우터를 이용한 기법이고, 나머지 하나는 서비스품질보장 기술을 이용한 기법이다[6-14].

전자의 경우 Rocky K. C. Chang가 제시한 기법[6]으로 분산서비스거부 공격에 대응하기 위하여 비정상 트래픽을 전송하는 근원지와 공격대상 호스트 사이에 존재하는 각각의 라우터들에서 비정상 트래픽을 차단하는 방식이다. 이는 대량의 비정상 트래픽을 보내는 근원은 깔때기의 맨 상단에 위치하고, 최종 공격대상 호스트는 깔때기의 맨 하단에 도착하기 때문에 분산된 지역에서 전송된 비정상 트래픽은 최종 공격대상 호스트에 도착할 때에는 동시에 많은 양의 비정상 트래픽으로 전달되기에 분산서비스거부 공격이 가능하다고 이야기한다. 이를 방지하기 위해서는 비정상 트래픽을 전송하는 근원지에 위치한 라우터에서부터 최종 공격대상 호스트 전에 위치한 라우터까지 단계적으로 비정상 트래픽에 해당하는 트래픽을 차단함으로써 점진적으로 증대되는 분산서비스거부 공격을 차단할 수 있다고 이야기하고 있다.

후자의 경우 Frank Kargl[7]이 제시한 기법으로 분산서비스거부 공격으로부터 웹서버를 보호하기 위하여 공격 가능성이 있는 트래픽이 통과하는 네트워크 대역폭을 점차적으로 낮춤으로써 최종적으로 방화벽에서 해당 트래픽을 차단하는 방식으로 동작한다. 이에 사용된 서비스품질보장 기술은 리눅스에서 지원하는 다양한 서비스품질보장 기술[8] 중에서 Class Based Queuing (CBQ)를 사용하였다. 이러한 기법으로 실험 환경을 구성하고 실험 결과를 보임으로

써 분산서비스거부 공격 중에도 효과적으로 정상 서비스를 제공할 수 있다고 설명한다.

위에서 설명한 두 가지 기법들은 모두 저자의 생각과 실험 결과만을 제시하고 있을 뿐, 왜 좋은지에 대한 설명과 구체적으로 어떠한 조건에서 가장 좋은 효과적인지에 대한 근거는 제시하지 못하였다. 이에 본 논문에서는 단계적 대응 기법을 이론적으로 정의하여 이원적 대응 기법과 비교하고, 가장 효과적인 조건을 제시함으로써 웜과 같은 대량의 비정상 트래픽을 발생시키는 공격에서 단계적 대응 기법이 효과적임을 보이도록 한다.

Ⅲ. 단계적 대응 기법 및 시스템

본 장에서는 본 논문에서 사용되는 단계적 대응 기법, 비정상 트래픽, 그리고 네트워크 트래픽이라는 세 가지 개념에 대해서 상세히 설명하고, 웜에 의해 발생된 비정상 트래픽을 효과적으로 대응할 수 있는 네트워크 대역폭 조절 방식의 단계적 대응 시스템 설계 내용을 보인다.

1. 단계적 대응 기법

단계적 대응 기법이란 특정 네트워크로 유입되는 트래픽에 대해 비정상 트래픽 여부를 확인하기 위하여 비정상 트래픽 탐지 루틴을 다수 통과하도록 함으로써, 해당 트래픽이 비정상 트래픽일 가능성이 가장 높았을 경우에 비정상 트래픽으로 판단하는 기법으로 정의한다[15,16]. 즉, 비정상 트래픽일 가능성이 가장 높은 트래픽을 비정상 트래픽으로 판단하여 차단하기 전까지는 모든 트래픽을 '단지 의심되는 비정상 트래픽'으로써 해당 네트워크를 통과하도록 하는 기법이다. 이러한 기법이 동작하기 위해서는 세 가지 전제조건이 필요하다. (1) 비정상 트래픽 탐지 루틴은 매우 짧은 시간동안에 해당 트래픽의 비정상 여부를 판단할 수 있어야 한다. 이는 비정상 트래픽 탐지 루틴을 다수 통과시키는 동안 웜에 의한 피해가 발생하지 않아야 하기 때문이다. (2) 최종적으로 차단되어야하는 비정상 트래픽으로 판단되기 전까지 해당 트래픽은 정상 트래픽처럼 해당 네트워크를 이용하도록 한다. 이는, 최종적으로 비정상 트래픽으로 판단되기 전까지 해당 트래픽은 정상 트래픽으로 복원될 가능성이 존재하기 때문이다. (3) 비정상 트래픽 탐지 루틴을 통과하는 회수를 최소화한다. 이는 시스템에 과도한 부하를 주지 않도록 하기 위해서일 뿐 만 아니라, 웜에 의한 피해가 발생하지 않도록 하기 위함이다.

위에서 언급한 세가지 전제조건을 기반으로 비정상 트래픽에 대해 단계적 대응을 실시하는 방식은 다음과 같다. 먼저 시스템이 운영되는 동안 정상 트래픽과 비정상 트래픽이 각각 통과할 수 있는 네트워크 대역폭을 고정 할당한 다음, 정상 트래픽이 비정상 트래픽 탐지 루틴에 의해서 비정상 트래픽으로 의심되었을 경우에는 해당 트래픽의 대역폭을 조절하여 비정상 트래픽이 통과하도록 지정된 네트워크 대역폭을 이용하도록 하며, 이미 비정상 트래픽으로 의심되어 대역폭이 조절된 트래픽이 다시 비정상 트래픽 탐지 루틴에 의해서 비정상으로 판단되었을 경우에는 해당 트래픽을 차단한다. 만일 이미 네트워크 대역폭이 조절되었던 트래픽이 비정상 탐지 루틴에 의해서 잘못된 판단으로 결정되었을 경우에는 정상 트래픽용 네트워크 고정 대역폭을 이용할 수 있도록 해당 트래픽의 대역폭을 조절한다. 이러한 단계적 대응 기법의 동작 방식에 대한 네트워크 트래픽 상태 전이도는 그림 1과 같다.

특정 네트워크를 통과하는 트래픽이 가질 수 있는 상태로는 정상 트래픽이 통과할 수 있는 정상우선순위

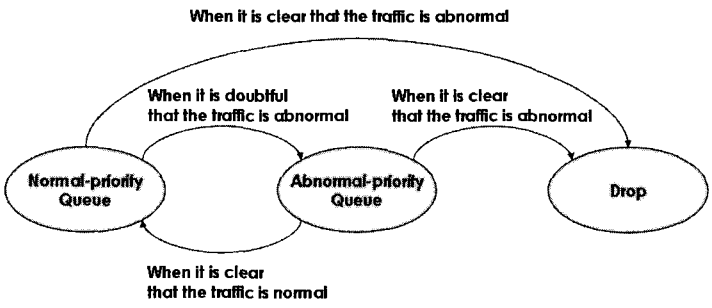

그림 1. 네트워크 트래픽 상태전이도

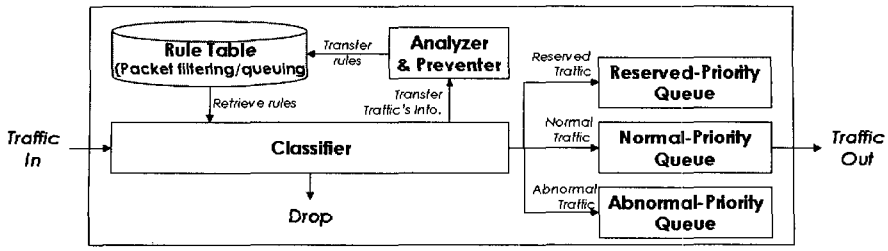

그림 2. 단계적 대응 시스템 구조도

큐 (Normal-priority Queue) 상태, 비정상으로 의심되는 트래픽이 통과할 수 있는 비정상우선순위 큐 (Abnormal-priority Queue) 상태, 그리고 비정상 트래픽으로 판단되었을 경우에 적용되는 차단 (Drop) 상태가 있다. 정상우선순위 큐를 통과하는 트래픽 중에서 비정상 트래픽 시그너처와 일치하는 트래픽이 존재할 경우에는 바로 차단 상태로 전이된다.

2. 비정상 트래픽 및 네트워크 트래픽

본 논문에서는 비정상 트래픽이란 네트워크에 존재하는 트래픽 중에서 웜에 의해 단시간동안 발생하는 대량의 트래픽으로 정의하며, 일반적으로 정상적인 사용자의 네트워크 트래픽 이외의 모든 네트워크 트래픽을 의미한다. 이러한 비정상 트래픽이 가지는 특징으로서는 크게 아래와 같이 세 가지가 있다.

- 주소위장 기법을 사용하여 공격자의 IP 주소를 위장한다.
- 취약 호스트들에 대한 공격을 먼저 실시하여 주 공격에 필요한 조건을 형성한다.
- 단시간동안 대량의 비정상 트래픽이 발생하도록 한다.

위에서 언급한 비정상 트래픽이 가지는 세 가지 특징 중에서 본 논문에서는 세 번째 특징만을 가지는 트래픽만을 고려하고자 한다. 그 이유로는 트래픽의 주소위장여부를 확인할 수 있는 다양한 연구가 수행되고 있으나, 다양한 웜 종류별로 주소가 위장된 비정상 트래픽 비율을 정확히 예측하기 어렵고, 주공격이 발생하기 전에 이뤄지는 취약 호스트들에 대한 공격은 비교적 긴 시간이 소요되며, 이에 대한 성공률을 확인할 수 없기 때문이다. 따라서 본 논문에서 비정상 트래픽이 가지는 특징 중에서 세 번째 특징인

단시간 동안 대량의 비정상트래픽이 발생하는 경우에 한해서만 단계적 대응 기법을 적용할 수 있다.

또한 일반적으로 네트워크 트래픽이라 함은 연속시간 관점에서 패킷의 흐름을 의미하지만, 트래픽을 분석하기 위해서는 일정 시간동안의 트래픽을 대상으로 분석하는 것이 편리하기 때문에, 본 논문에서는 네트워크 트래픽이란 이산시간 관점에서 패킷의 흐름으로 정의한다. 또한 임의의 시각 i에 비정상 트래픽 탐지 루틴이 τ 동안 동작하고, $i+1$에 비정상 트래픽 탐지 루틴이 다시 τ 동안 동작한다는 전제하에서 비교 분석을 실시한다.

3. 단계적 대응 시스템

단계적 대응 기법이 적용된 단계적 대응 시스템 구조도는 그림 2와 같다. 단계적 대응 시스템은 보호하고자 하는 네트워크 또는 시스템 앞단에 설치되거나 네트워크 진입지점에 설치될 수 있기 때문에 네트워크 대역폭의 성능을 저하시키지 않도록 동작하여야 한다.

단계적 대응 시스템은 크게 세 가지 모듈로 구성되어 있다. 각 모듈은 규칙 테이블 및 분류기(rule table & classifier), 분석 및 대응기(analyzer & preventer), 그리고 예약/정상/비정상 우선순위 큐(reserved/normal/abnormal-priority queue)이다. 트래픽이 도착하면 먼저 분류기에서 규칙 테이블에 정의된 규칙들을 기반으로 해당 트래픽을 필터링하거나 우선순위 큐로 통과하도록 하며, 정의된 규칙이 없거나 정상 우선순위 큐를 통과하는 트래픽의 경우에는 해당 트래픽의 비정상 유무를 분석하기 위하여 트래픽 정보를 분석 및 대응기로 전달한다. 트래픽 정보를 전달받은 분석 및 대응기는 비정상 우선순위 큐를 통과하는 트래픽이 다시 비정상으로 판단되었을 경우에는 필터링 규칙을, 정상 우선순위 큐를 통과하는 트래픽이 비정상으로 의심되었을 경우에는 서비스품질보장 규칙을 생성하여 규칙 테이블에 저장하는 방식으로 동작한다. 이 경우 분석 및

표 1. 단계적 대응 시스템 구성 모듈

구분		설 명
규칙 테이블 및 분류기 (rule table & classifier)		· 수신한 트래픽들을 '분석 및 대응기'로 전달 · '규칙 테이블'의 트래픽 필터링 규칙을 참조하여 비정상 네트워크 트래픽 차단 · '규칙 테이블'의 서비스품질보장 규칙을 참조하여 네트워크 트래픽의 서비스품질 조절
분석 및 방어기 (analyzer & preventer)		· '분류기'가 전달한 트래픽의 정보를 보안 관리자가 사전에 설정에 보안 정책에 따라 분석 · 분석된 트래픽의 정보를 기반으로 비정상 트래픽으로 판단된 트래픽을 차단하기 위한 트래픽 필터링 규칙 생성 · 분석된 트래픽의 정보를 기반으로 비정상 트래픽으로 의심되는 트래픽의 서비스품질을 조절하기 위한 서비스품질보장 규칙 생성
우선순위 큐	예약 우선순위 (reserved-priority)	· 예약 트래픽이 통과하는 큐 (예: 이메일, 웹서비스 등)
	정상 우선순위 (normal-priority)	· 정상 트래픽이 통과하는 큐
	비정상 우선순위 (abnormal-priority)	· 비정상 트래픽으로 의심되는 트래픽이 통과하는 큐

대응기가 트래픽의 비정상 유무를 판단하는 기준은 보안 관리자가 설정한 보안 정책에 따르며, 우선순위 큐들도 보안 관리자가 사전에 설정한 정보를 참조하여 동작한다. 단계적 대응 시스템의 각 모듈이 수행하는 기능은 표 1과 같다.

그림 2에서 보인 단계적 대응 시스템을 구성하는 세 가지 모듈인 규칙 테이블 및 분류기, 분석 및 대응기, 그리고 예약/정상/비정상 우선순위 큐을 구현할 경우 다음과 같은 특성을 고려할 수 있다.

· 규칙 테이블 및 분류기

규칙 테이블은 '분석 및 대응기'에서 생성한 필터링 규칙 및 큐잉 규칙을 보관하고 있으며, 시스템이 운영됨에 따라 증가하는 규칙들을 기반으로 τ 마다 네트워크로 유입되는 트래픽을 효과적으로 처리하기 위해서 분류는 효과적인 규칙 매칭 알고리즘을 가져야 한다. 또한 단계적 대응 기법이 OSI 7 계층의 네트워크 계층 정보를 기반으로 동작할 경우에는 출발지와 도착지 IP 주소를 기반으로 분류기가 동작하여야 하며, 상위 계층의 정보를 기반으로 트래픽의 비정상 유무를 탐지할 경우에도 네트워크 계층에서 상위 계층의 정보를 한꺼번에 확인할 수 있는 구조를 가져야 한다.

· 분석 및 대응기

단계적 대응 기법은 임의의 시각 i에 통과하는 트래픽 정보를 기반으로 $i+1$와 $i+2$를 통과하는 트래픽에 대응하는 방식으로 동작하기 때문에 '분석 및 대응기'는 τ 동안 비정상 유무를 판단할 수 있어야 하며, i, $i+1$, 그리고 $i+2$ 시각에 특정 트래픽들에 대한 분석과 판단 및 대응을 동시에 처리하기 위해서는 트래픽의 상태정보를 보관하고 있어야 한다. 또한, τ 동안 통과하는 트래픽을 특정 저장 공간에 보관시켜 트래픽의 흐름을 정지시키는 것보다는 통과시키면서 분석 및 대응하는 것이 해당 네트워크를 보다 효율적으로 운영하는 방법일 것이다.

· 예약/정상/비정상 우선순위 큐

예약/정상/비정상 우선순위 큐는 그림 1과 2의 내용을 기반으로 다음과 같이 구성할 수 있다. 먼저 예약 우선순위 큐는 '분석 및 대응기'가 비정상적으로 동작하여 정상 우선순위 큐가 정상적인 서비스를 제공하지 못할 경우에도 최소한의 서비스를 제공하기 위한 용도로 사용된다. 이를 위하여 최소한의 단계적 대응 시스템에 의해 보호되고 있는 네트워크 또는 시스템을 제어할 수 있는 최소한의 네트워크 트래픽만 보장하면 된다. 또한, 정상 우선순위 큐는 전체 네트워크 대역폭의 절반 이상을 차지하도록 구성할 수 있지만, 이는 단계적 대응 시스템을 구현하는 방식에 따라서 정상 우선순위 큐가 차지하는 네트워크 대역폭의 비율이 달라질 수 있으며, 적용하고자 하는 네트워크의 특성에 의해서도 달라질 수 있다. 이에 대한 구체적인 내용에 대해서는 본 논문에서 설명하지 않기로 한다.

Ⅳ. 이원적 대응 기법과 단계적 대응 기법간 비교

본 장에서는 정상 트래픽 비율과 오탐지 트래픽 비율을 기준으로 이원적 대응 기법과 단계적 대응 기법과의 비교 내용을 보이고자 한다. 분석을 위해 사용된 트래픽에 대한 정의는 표 2와 같다.

표 2. 정상 트래픽, 비정상 트래픽, 그리고 오탐지 트래픽에 대한 정의

구 분	정 의	설 명
정상 트래픽 (N_i)	$\left\{N_{i,k} \mid \sum_{k=1}^{n} load\ of\ N_{i,k} \le NBW\right\}$	- NBW: 네트워크 대역폭 - N_i: τ 동안(=$[i, i+1)$) 통과하는 정상 트래픽
비정상 트래픽 (A_i)	$T_i - N_i$	- T_i: τ 동안 네트워크를 최대로 통과할 수 있는 트래픽 - A_i: τ 동안 T_i에서 N_i를 제외한 트래픽
오탐지 트래픽 (F_i)	$pA_i (0 \le p \le 1)$	τ 동안 A_i에서 확률 p만큼 오탐지(False-Positive)된 트래픽 (p는 비정상 트래픽 탐지 루틴에 따라서 상이함)

표 2에서 보이는 바와 같이 고정된 네트워크 대역폭 NBW에서 τ 동안 특정 네트워크를 통과하는 전체 트래픽은 T_i(수식 전개의 편의를 위하여 $NBW = T_i$로 정의함), 정상 사용자들의 트래픽 합을 N_i, T_i에서 N_i를 제외한 부분을 A_i라고 정의한다. 이 경우 N_i와 A_i가 가질 수 있는 값의 범위는 각각 $[0, T_i]$이다. 오탐지된 트래픽 F_i는 $F_i = pA_i (0 \le p \le 1)$를 만족한다. 따라서 임의의 시각 i에 네트워크를 최대로 통과할 수 있는 트래픽은 $T_i = N_i + (1-p)A_i + F_i$ $(0 \le p \le 1)$을 만족한다. 본 논문에서는 특정 네트워크에서의 정상 트래픽 비율과 오탐지 트래픽 비율을 각각 $\rho_i = \frac{N_i}{T_i}$와 $\theta_i = \frac{F_i}{T_i}$로 표현한다.

1. 정상 트래픽 비율

비정상 트래픽 탐지 루틴이 τ 동안 해당 네트워크로 유입되는 트래픽에 대하여 비정상 트래픽 여부에 대한 판단을 실시한 경우, 각각 α_i(T_i에서 N_i이 차지하는 트래픽 비율)와 β_i(T_i에서 A_i에 해당하는 트래픽 비율)의 비율로 존재한다. 따라서 τ 동안 T_i에서 N_i, A_i, 그리고 F_i가 존재하는 비율은 각각 $N_i = \alpha_i$, $A_i = (1-p)\beta_i$, 그리고 $F_i = p\beta_i$와 같다. 임의의 시각 i에 통과하는 트래픽에 대해서 이원적 대응 기법을 적용할 경우, 각각의 트래픽이 차지하는 비율은 표 3과 같다.

표 3에서 $i+1$에 A_{i+1}과 F_{i+1}이 0이 되는 이유는 비정상 트래픽 탐지 루틴이 동작하여 해당 트래픽을 모두 차단하였기 때문이다. 이에 반하여 단계적 대응 기법을 적용할 경우, τ 동안 해당 네트워크로 유입되는 트래픽의 네트워크 대역폭을 각각 α(T_i에서 N_i에 할당된 네트워크 대역폭 비율)와 β(T_i에서 A_i에 할당된 네트워크 대역폭 비율)의 비율로 각각 할당하면, τ 동안 N_i와 A_i가 존재하는 비율은 각각 해당 트래픽에게 할당된 네트워크 대역폭 비율인 α와 β이다. (단, α와 β는 대응이 시작되기 전에 정적으로 설정되는 값이기 때문에 $\alpha : \beta = \alpha_i : \beta_i$ $(0 < i)$을 유지한다.) 임의의 시각 i에 통과하는 트래픽들에 대해서 비정상 트래픽 탐지 루틴이 동작하여 단계적 대응을 실시할 경우, 각각의 트래픽이 차지하는 비율은 그림 3 및 표 4와 같다.

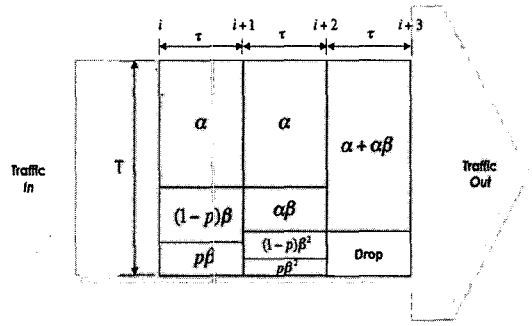

그림 3. 단계적 대응 기법을 적용하였을 경우, 임의의 시각 i, $i+1$, 그리고 $i+2$에 존재하는 트래픽별 비율(b)

표 3. 이원적 대응 기법을 적용하였을 경우, 임의의 시각 i와 $i+1$에 존재하는 트래픽별 비율

	i	$i+1$
N	α_i	α_{i+1}
A	$(1-p)\beta_i$	0
F	$p\beta_i$	0

표 4. 단계적 대응 기법을 적용하였을 경우, 임의의 시각 i, $i+1$, 그리고 $i+2$에 존재하는 트래픽별 비율 (a)

	i	$i+1$	$i+2$
N	α	$\alpha+\alpha\beta$	$\alpha+\alpha\beta$
A	$(1-p)\beta$	$(1-p)\beta^2$	0
F	$p\beta$	$p\beta^2$	0

그림 3과 표 4에서 i에 단계적 대응을 실시한 후 $i+1$에 다시 단계적 대응을 실시하는 2단계 단계적 대응 기법을 적용할 경우를 보이며, $i+2$에 A_{i+2}와 F_{i+2}가 0이 되는 이유는 표 3과 같다. 표 3과 4를 기준으로 이원적 대응 기법과 단계적 대응 기법을 적용할 경우에 대해 정상 트래픽 비율을 비교하면 다음과 같다. 전자의 경우, 임의의 시각 i에서 모두 N_i의 비율은 α_i이므로 정상 트래픽 비율(ρ_i)은 수식 1과 같다.

$$\rho_i = \frac{N_i}{T_i} = \alpha_i \tag{1}$$

그러나 단계적 대응의 경우 평균 정상 트래픽 비율(ρ)은 수식 2와 같다.

$$\rho = \frac{N_i}{T} + \frac{N_{i+1}}{T} = \frac{1}{2}(\alpha + \alpha + \alpha\beta)$$
$$(\text{단, } \alpha+\beta=1) \tag{2}$$

수식 2에서 α를 기준으로 정리하면 정상 트래픽 비율은 $\rho = -\frac{1}{2}(\alpha - \frac{3}{2})^2 + \frac{9}{8}$ $(0 \le \alpha \le 1)$을 만족한다. 수식 1과 2를 그래프로 표현하면 그림 4와 같다.

그림 4에서 보이는 바와 같이 임의의 시각 i에 비정상 트래픽 탐지 루틴이 동작하여 탐지 순간의 트래픽별 대역폭을 차지하는 비율을 기반으로 비교하였을 때, 전체적으로 단계적 대응 기법을 적용한 경우 α에 상관없이 ρ가 높음을 알 수 있다. 또한 (1)과 (2)간에 가장 큰 차이를 보이는 α를 확인하면 $\alpha = 0.5$ ($\frac{d\rho}{d\alpha} = -\alpha + \frac{1}{2}$)가 됨을 확인할 수 있다. 이는 단계적 대응 기법을 사용할 경우, 임의의 i에서는 이원적 대응 기법과 동일한 정상 트래픽 비율을 가진다. 그러나 $i+1$에서 비정상 트래픽 β 중 비정상 트래픽 탐지 루틴에 의해서 정상 트래픽으로 판단된 $\alpha\beta$만큼 정상 트래픽 비율은 증가하기 때문에 평균 정상 트래픽 비율은 $\frac{1+\beta}{2}$만큼 증가한다.

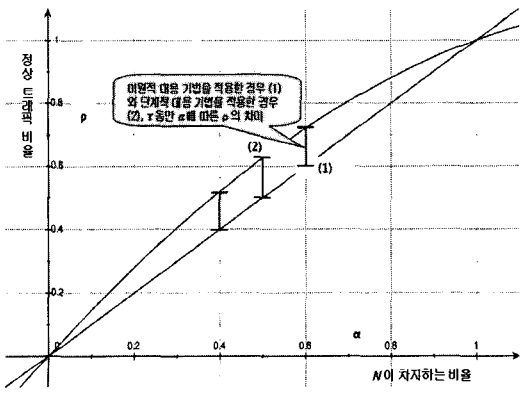

그림 4. 이원적 대응 기법을 적용한 경우(1)와 단계적 대응 기법을 적용한 경우 (2)에서 α에 대한 정상 트래픽 비율 (ρ)

2. 오탐지 트래픽 비율

표 3과 4를 기준으로 오탐지 트래픽 비율을 비교하면 다음과 같다. 이원적 대응 기법을 적용할 경우, 임의의 시각 i에서 F_i의 비율은 $p\beta_i$이므로 오탐지 비율 (θ_i)은 수식 3과 같다.

$$\theta_i = \frac{F_i}{T_i} = p\beta_i \tag{3}$$

그러나 단계적 대응 기법을 적용한 경우 평균 오탐지 트래픽 비율 (θ)은 수식 4와 같다.

$$\theta = \frac{F_i}{T} + \frac{F_{i+1}}{T} = \frac{1}{2}(p\beta + p\beta^2)$$
$$(\text{단, } \alpha+\beta=1) \tag{4}$$

수식 4에서 α를 기준으로 정리하면 오탐지 트래픽 비율은 $\theta = \frac{p}{2}(\beta^2 + \beta)$ $(0 \le \beta \le 1)$을 만족한다. 수식 3과 4를 그래프로 표현하면 그림 5와 같다.

그림 5에서 보이는 바와 같이 임의의 시각 i에 비정상 트래픽 탐지 루틴이 동작하여 탐지 순간의 트래픽별 대역폭을 차지하는 비율을 기반으로 비교하였을 때, 단계적 대응 기법을 적용할 경우 전체적으로 β에 상관없이 θ가 낮음을 알 수 있다. 또한 (3)과 (4)간에 가장 큰 차이를 보이는 β를 확인하면 p에 상관없이 $\beta = 0.5$ ($\frac{d\theta}{d\beta} = -\beta + \frac{1}{2}$)가 됨을 확인할 수 있다. 이는 단계적 대응 기법을 사용할 경우, 임의의 i에서는 이원적 대응 기법과 동일한 오탐지 트래픽 비율을 가지지만, $i+1$에서 비정상 트래픽 β 중에서 비정상 트래픽 탐지 루틴에 의해 탐지되는 오탐지 트래픽 비

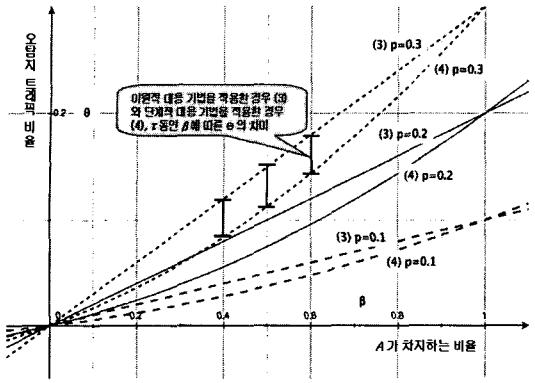

그림 5. 이원적 대응 기법을 적용한 경우 (3)와 단계적 대응 기법을 적용한 경우 (4)에서 β에 대한 오탐지 트래픽 비율 (θ)

율은 $p\beta^2$이 되기 때문에 평균 오탐지 트래픽 비율은 $\frac{1+\beta}{2}$만큼 감소한다.

V. 결 론

본 논문에서는 웜과 같은 악의적인 프로그램에 의해서 단시간동안 발생한 대량의 비정상 트래픽에 대응하기 위한 기법 중에서 트래픽 필터링 기반의 비정상행위 탐지 방식으로 동작하는 대응 기법과 네트워크 대역폭을 조절하는 방식의 단계적 대응 기법을 이론적으로 비교하였다. 비교 기준은 네트워크를 통과하는 정상 트래픽 비율과 오탐지 트래픽 비율로 하였으며, 임의의 시간 동안 전체 네트워크 트래픽에서 비정상 트래픽이 차지하는 비율을 β라고 할 경우, 단계적 대응 기법의 평균 정상 트래픽 비율은 $(1+\beta)/2$만큼 증가하고, 평균 오탐지 트래픽 비율은 $(1+\beta)/2$만큼 감소한다.

이러한 단계적 대응 기법을 이용하여 단계적 대응 시스템을 구성할 경우, 크게 규칙 테이블 및 분류기, 분석 및 대응기, 그리고 예약/정상/비정상 우선순위 큐로 구분하여 설계할 수 있다. 규칙 테이블 및 분류기는 실시간으로 네트워크로 유입되는 트래픽을 규칙 테이블과 비교하기 위한 효율적인 규칙 매핑 알고리즘을 사용해야 하고, 단시간동안 대량의 트래픽을 발생시키는 웜의 특성을 감안하여 분석기 및 대응기를 설계하여야 한다. 또한, 최악의 경우 최소한의 서비스를 제공하기 위한 예약 우선순위 큐와 전체 네트워크 대역폭의 절반 이상을 차지하는 정상 우선순위 큐를 고려하여 단계적 대응 시스템을 설계할 수 있다.

참 고 문 헌

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

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

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

[4] CERT/CC, "CERT Advisory CA-2001-26 Nimda Worm," http://www.cert.org/ad visories/ CA-2001-26.html, Sept. 2001.

[5] D. Song, R. Malan, and R. Stone, "A Snapshot of Global Internet Worm Activity," Technical Report, Arbor Networks, Nov. 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. 42-51O, ct. 2002.

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

[8] Linux Advanced Routing HOWTO, http://www.linuxdoc.org/.

[9] 전용희, "침입방지시스템(IPS)의 기술 분석 및 성능평가 방안," 정보보호학회지 Vol. 15, No. 2, pp. 63-73, 2005.

[10] 조태남, 이상호, "(2,4)-트리를 이용한 그룹키 관리," 정보보호학회논문지 Vol. 11, No. 4, pp. 64-77, 2001.

[11] 박영호, 이경현, "이동네트워크 환경에서 그룹키 관리구조," 정보보호학회논문지 Vol. 12, No. 2, pp. 77-89, 2002.

[12] 권정옥, 황정연, 김현정, 이동훈, 임종인, "일방향 함수와 XOR을 이용한 효율적인 그룹키 관리 프로토콜: ELKH," 정보보호학회논문지 Vol. 12, No. 6, pp. 93~112, 2002.
[13] 이상원, 천정희, 김용대, "Pairing을 이용한 트리 기반 그룹키 합의 프로토콜," 정보보호학회논문지 Vol. 13, No. 3, pp. 101~110, 2003.
[14] 박영희, 정병천, 이윤호, 김희열, 이재원, 윤현수, "Diffie-Hellman 키 교환을 이용한 확장성을 가진 계층적 그룹키 설정 프롤콜," 정보통학회논문지 Vol. 13, No. 5, pp. 3~15, 2003.
[15] K. Ko, E. Cho, T. Lee, Y. Kang, and Y. I. Eom, "The Abnormal Traffic Control Framework based on QoS Mechanisms," Lecture Notes in Computer Science 3280, pp. 167-175, Oct. 2004.
[16] J. Kim, K. Ko, Y. Kang and Y. I. Eom, "Stepwise Intrusion Prevention based on Abnormal Traffic Control Framework," Proc. of the 4th International Conference on Asian Language Processing and Information Technology (ALPIT 2005), pp. 77-82, Jun. 2005.

〈著者紹介〉

고 광 선 (Kwangsun Ko) 학생회원
1998년 2월: 성균관대학교 정보공학과 졸업
2004년 8월: 성균관대학교 전기전자및컴퓨터공학부 석사
2004년 9월~현재: 성균관대학교 컴퓨터공학과 박사과정
〈관심분야〉 정보보호, 리눅스, 네트워크

강 용 혁 (Yong-hyeog Kang) 정회원
1996년 2월: 성균관대학교 정보공학과 졸업
1998년 2월: 성균관대학교 정보공학과 석사
2004년 8월: 성균관대학교 전기전자및컴퓨터공학과 박사
2004년 3월~현재: 극동대학교 경영학부 정보경영학과 교수
〈관심분야〉 전자상거래, 시스템 보안, 네트워크 보안, 리눅스

엄 영 익 (Young Ik Eom) 종신회원
1983년 2월: 서울대학교 계산통계학과 졸업
1985년 2월: 서울대학교 전산과학과 석사
1991년 8월: 서울대학교 전산과학과 박사
2000년 9월~2001년 8월: Dept. of Info. and Comm. Science at UCI 방문교수
1993년 3월~현재: 성균관대학교 정보통신공학부 교수
〈관심분야〉 분산 컴퓨팅, 이동 컴퓨팅, 이동 에이전트, 시스템 보안, 운영체제, 내장형 시스템