인터넷 액세스점에서의 이상 트래픽 제어기 성능분석

정회원 김 광 식

Analysis of abnormal traffic controller deployed in Internet access point

Kwangsik Kim* *Regular Member*

요 약

본 논문에서는 네트워크의 생존성을 보장하고 신뢰성 높은 인터넷 서비스를 제공하기 위한 차세대 보안기술로서 인터넷의 액세스점에 위치하는 이상 트래픽 제어기(ATC, Abnormal Traffic Controller)를 제안한다. ATC의 주요 개념은 이상 트래픽 감지와 트래픽 제어기술에 있는데, 네트워크에서 에러의 요인이 계속 존재하거나 반복되는 경우 이상 트래픽 제어를 통해 서비스 완료성을 가능한 보장하는 것을 그 목적으로 한다 분석결과, 이상 트래픽 중 유효 트래픽의 비율이 30%를 초과하는 경우에는 이상 트래픽에 대한 제어정책을 사용하는 ATC는 기존의 네트워크 노드 뿐만 아니라 차단정책을 사용하는 ATC보다 우수한 성능을 나타내었다 과다 트래픽의 알려지지 않은 공격이 발생하는 경우, 높은 오탐지율로 인해 기존의 네트워크 IDS로는 한계가 있는데, 이러한 환경에서 ATC는 네트워크 노드를 도와서 이상 트래픽을 제어하는데 주요한 역할을 수행하게 된다

Key Words Abnormal traffic controller, Internet access point, traffic monitoring

ABSTRACT

ATC (Abnormal traffic controller) is presented as next generation security technology to securely support reliable Internet service and to guarantee network survivability, which is deployed in Internet access point. The key concept of the ATC is abnormal traffic monitoring and traffic control technology When fault factors exist continuously and/or are repeated, abnormal traffic control guarantees service completeness as much as possible The ATC with control policy on abnormal traffic is superior to the ATC with blocking policy as well as conventional network node, when the ratio of effective traffic to abnormal traffic is higher than 30% When traffic intended unknown attack occurs, network IDS is high false positive probability and so is limited to apply In this environment, the ATC can be a key player to help the network node such as router to control abnormal traffic.

Ⅰ. 서 론

최근에 사이버 공격의 추세는 단순한 시스템 공격에서 특정 서비스가 중단되는 네트워크 공격으로 변하고 있다 [1, 2]. 예를 들어, 인터넷 웜이 급속히 확산된 2003년도 1월 25일 인터넷 침해사고로 인해 서비스가 마비되는 사태가 발생했다 이를 통해 사이버 공격이 개별 사생활 침해를 넘어 국가적인 경제 손실뿐만 아니라 국가 보안 및 사회 질서를 위협하는 수준에 이르렀다 그러나, 기존의 보안기술은 인터넷 에러가 발생할 때 복구하는데 너무 많은 시간이 소요된다 이는 많은 패킷들이 패킷 타입에 관계없이 제거되고 정상 서비스 제공이 긴 에러 복구시간이 지나야 가능하기 때문이다

* 한국전자통신연구원 정보보호연구단(kks63453@etri re kr)
논문번호 #KICS2004-08-131, 접수일자 2004년 8월 4일

보안 측면에서, ISP 네트워크 접속점에서의 트래픽 모니터링과 제어기술은 사용자 서비스를 안전하게 고객망에서 백본망으로 지속적으로 전달하고 또한 해킹과 바이러스에 의한 침입에 따른 피해의 국지화 등을 통한 신속한 대응으로 네트워크의 생존성을 높이는 현실적인 해결책으로 부상하고 있다. 안전한 인터넷 서비스에 대한 대표적인 연구로는 DARPA FTN (Fault tolerant network) [3]과 Arbor Inc.사의 Peakflow [4]가 있다. Peakflow는 보안 관련 데이터를 측정하고, 모으고, 상관성을 분석할 때 CISCO의 netflow가 제공하는 트래픽 분석결과에 의존한다. 즉, CISCO 라우터가 존재하는 환경에서만 적용할 수 있다.

본 논문에서는 안전한 인터넷 서비스 제공을 위한 차세대 보안기술로서 ATC (Abnormal traffic controller)를 제안한다. 외부의 공격, 침입과 취약성과 같은 에러 요인들이 존재하는 곳에서도 ATC는 선 정의된 품질기준에서 서비스를 유지하는 것을 가능하게 한다. 과다 트래픽을 통한 알려지지 않은 공격이 발생할 때, 네트워크 IDS에서의 오탐지율은 높아지게 되고, 이에 따라 탐지결과는 무용지물이 될 수 있다. 이러한 환경에서 ATC는 라우터와 같은 네트워크 노드를 도와서 이상 트래픽을 다루는데 주요한 역할을 담당할 수 있다. ATC의 주 개념은 이상 트래픽 모니터링과 트래픽 제어 기술에 있다. 에러 요인이 지속적으로 존재하고 반복되는 환경에서도, 이상 트래픽 제어를 통하여 가능한 서비스 완료율을 높일 수 있다.

본 고는 다음과 같이 구성된다. 다음 장에서 ATC의 개념을 소개한다. 트래픽 모델이 3장에서 소개되고 4장에서 성능 측정 방법이 제시된다. 5장에서는 ATC 방식에 의해 가질 수 있는 성능개선 효과를 설명하고 6장에서 결론을 맺는다.

II. 제안 방식

1. ATC 프레임워크

본 장에서는 ATC 프레임워크를 소개하고자 한다. ATC는 에러를 국지화하고 네트워크 생존성을 높이기 위해 이상 트래픽 모니터링과 트래픽 제어 기술을 사용한다. 이를 통해 에러 요인이 지속적으로 존재하고 반복될 때에도 서비스 완료율을 가능한 높이도록 한다. 그림 1에서 보는 바와 같이 ATC 프레임워크는 2가지 단계로 구분된다.

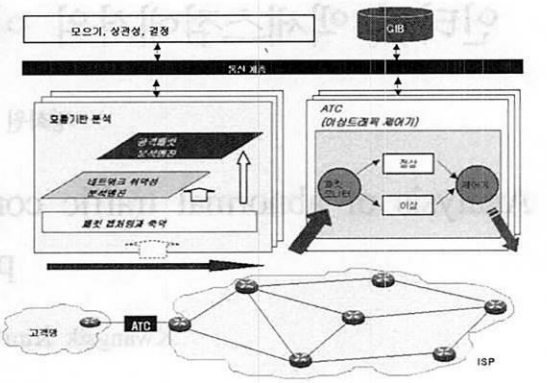


그림 1. ATC 프레임워크

첫 단계는 흐름 기반 트래픽 분석 단계이다. 이 단계는 다시 인터넷 서비스 에러에 대한 예방적 행위를 위한 네트워크 취약성 분석 엔진과 에러 사건 시간을 짧게 하기 위한 이상 트래픽 제어를 위한 공격 패킷 분석 엔진으로 구성된다. 두번째 단계는 이상 트래픽 제어 단계이다. 이 단계는 다시 흐름기반 트래픽 분석을 통한 패킷 모니터링과 이상 트래픽에 대한 적절한 행위를 수행하는 부분으로 구성된다. GIB (Global information base)는 패킷정보를 모으고 상관성을 분석하고 대응방식을 결정하게 된다. 또한 패킷, 사용자 및 사이트 정보를 관리한다. 흐름기반 트래픽 분석 결과는 GIB를 통하여 ATC에 보내지게 되는데, 본 논문에서는 ATC가 흐름기반 트래픽 분석을 통하여 이상 트래픽 제어기능을 수행한다고 가정한다.

2. 제안된 서비스 모델

최근에는 알려지지 않은 공격이 종종 일어나고 있는데, 미래에는 일상적인 것이 될 것이다. 알려지지 않은 공격의 경우에 IDS, IPS 및 보안어플라이언스와 같은 보안 장비들은 고객망과 접속하는ISP 인입점의 트래픽에 대하여 오탐지를 할 수 있다. 보안 장비는 이상 트래픽을 막을지 아니면 통과시킬 지에 대해 어려움을 가지게 된다. 왜냐하면, 이상 트래픽의 일부는 유효 트래픽이기 때문이다. 여기서 유효 트래픽은 오염된 트래픽이 아닌 인터넷 사용자에 의해 발생된 실제 트래픽을 의미한다. 그림 2에서 보는 바와 같이 제안된 ATC는 이상 트래픽 중에서 유효 트래픽을 보호하기 위해 이상 트래픽에 대한 소프트 방화벽 기능의 보안 정책을 수행한다.

ATC는 ADSL 기술을 사용하는 가입자 망에서 DSLAM과 같은 액세스망 노드 근처에 위치할 수 있다. ATC는 일종의 전처리 프로세서이며 네트워크 노

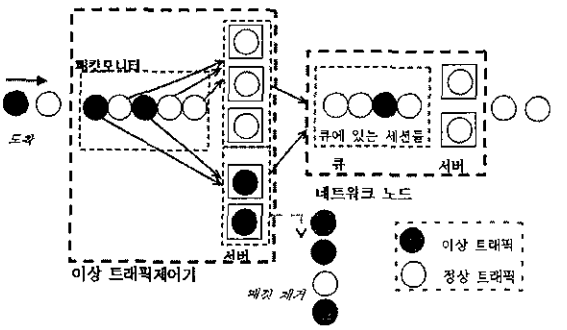


그림 2 ATC 서비스 모델

드에 플러그인 형태나 독립적인 시스템으로 운영될 수 있다. 세션들은 전화망에서의 채널처럼 가상 채널 연결에 의해 서비스 된다고 하자. 그리고 ATC는 세션 당 가상 연결의 시작과 끝 시점을 모니터링하고 있다고 하자. 이러한 경우 트래픽 모델은 Erlang loss 모델로 근사될 수 있다.

그림 2에서 패킷 모니터는 흐름기반 패킷모니터링을 수행한다. 만일 패킷이 오염된 패킷으로 의심 된다면 이상 트래픽으로 간주한다. 이상 트래픽에 후순위를 줌으로써 이상 트래픽을 제어하는데, 제어 정책은 차단이나 전송속도제한이 될 수 있다. 이와 같이 함으로서, 오염된 패킷은 낮은 생존율을 가지게 되고 전체 유효전송률은 증가하게 될 것이다.

III. 성능분석모델

본 장에서는 제안 방식의 수학적 모델을 제안한다. 품질보장이 요구되는 주요 서비스를 위해서 미래에는 액세스망 노드에서 가상 채널 서비스를 사용하는 것은 일상적이 될 것이다. 그리고 세션들은 전화망 채널처럼 가상 채널 연결에 의해 서비스된다. 참고문헌 [5]에서는 WAN 환경에서 WWW 또는 FTP 세션의 도착 사건은 고정 속도를 가진 포아송 프로세스로 잘 모델링이 된다고 한다. 그리고 세션지속시간은 Pareto 분포를 따른다고 한다. 따라서, 본 고에서는 세션지속시간은 지수분포 뿐만 아니라 Pareto 분포를 따르는 것을 고려한다.

1 세션의 도착과정

ATC는 무한한 세션 요청자가 있다는 가정하에 n 채널을 지원한다고 하자. 만일 세션이 도착하는 시점에 모든 n 채널이 사용 중이라면, 그 세션은 시스템에서 서비스 되는 대신에 소실되게 된다. 세션의 도착은 고정 속도를 가진 동차의 포아송 프로세스의 통계 특성을 근사화 하는 것으로 볼 수 있다. 포아송 프로세스는 재생 프로세스로 특징 지을 수 있는데, 아래의 식과 같이 도착 시점간 간격이 속도 파라미터인 λ를 가지는 지수 분포가 된다.

$$F(t)=1-e^{-\lambda t} \tag{3.1}$$

이때, ATC에서 성공적인 신규 세션 시도는 아래와 같이 주어진다.

$$\lambda_s=\lambda(1-P_b) \tag{3.2}$$

여기서, P_b는 신규 세션의 블록킹 확률이다.

2 세션 크기와 세션지속시간

세션을 구성하는 파일들의 크기는 통계적으로 어떻게 표현해야 할까? 통계적인 분석이 되기 위해서 세션은 시간축으로 변환되어야 한다. 1Mbits/s의 가상 채널이 사용되고 패킷 헤더, 패킷 ACK 등과 같은 세션의 오버헤드가 50%라고 가정하자. 이때, 표 1은 세션의 지속시간 값을 나타낸다.

표 1 세션 크기 구분

구분	세션 크기	세션지속시간
소	25 ~ 500 kbytes	0.4 ~ 8 s
중	0.5 ~ 5 Mbytes	8~ 80 s
대	5 ~ 25 Mbytes	80 ~ 400 s

세션지속시간은 파라미터 μ를 가지는 독립적 이면서 지수분포를 가지는 랜덤 변수이고, 세션 도착 과정에 독립적이다 라고 가정한다. 통계적인 분석의 용이성 때문에 세션지속시간 T_s를 지수분포로 고려한다. 즉, 세션지속시간은 평균이 $1/\mu$인 지수분포를 따르며, 이에 대한 PDF는 다음과 같다.

$$f(t)=\mu e^{-\mu t} \tag{3.3}$$

여기서, μ는 세션 서비스율이다.

더 현실적으로 말해서, 세션을 구성하는 데이터 파일의 전체적인 통계치는 Pareto 분포에 의해 잘 근사화 된다 [5,6]. 표 1에서 정의한 파일 크기의 3가지 범위를 수용하기 위하여 Pareto 분포를 수정하여 m 보다 더 큰 모든 값들은 절단하고, 이에 따라 PDF의 합친 밀도함수 값이 1이 되도록 조정한다. 절단된

Pareto 분포의 밀도함수는 다음과 같이 주어진다

$$f(t)=\begin{cases} 0, & \text{if } t<k,\ t>m \\ \dfrac{\alpha\times k^{\alpha}}{t^{\alpha-1}(1-(k/m)^{\alpha})}, & \text{if } k\le t\le m \end{cases} \quad (3\ 4)$$

여기서 m 은 분포의 가장 큰 값이고, k 는 가장 작은 값이다 α는 분포의 모양을 나타내는 파라미터이다 $(k/m)^{\alpha}$는 Pareto 분포와 차이가 나는 부분으로 조정 값이다 본 논문에서는 중간크기의 세션이 고려되는데, 그 시간길이는 음성 트래픽과 비슷하다 Pareto 분포에서, 세션지속시간은 표 2에서 보여지는 것과 같이 α 값을 고정함으로 해서 결정된다 [6].

표 2 평균 세션지속시간을 위한 α 값들

평균세션 지속시간	α 값	비고
20 s	1 87	가정 값 k=10 s, m=200 s
30 s	1 08	
40 s	0 66	
50 s	0 34	
60 s	0 08	

3. 채널 실패 사건과 복구 시간의 도착과정

채널 실패와 복구에 걸리는 시간은 각각 평균이 $1/\gamma$와 $1/\tau$인 지수분포를 따른다고 하자 또한 모든 채널은 하나의 복구 설비를 공유한다고 가정한다

4 이상 트래픽 특징들

이상 트래픽을 서비스하는 것이 좋은 방법인가? 네트워크 노드에서, 라인 속도는 매우 빠른데, 이에 따라 보안 관점에서 상세하게 입력 트래픽을 조사하는 것은 어렵다. 그래서, 인터넷 접속점에 위치하는 네트워크 노드의 보안 강도는 고객망에 놓이는 그것보다 약하다 현재 알려지지 않는 공격이 글로벌 네트워크 환경에서 일반적인 추세가 되어가고 있다 알려지지 않은 공격이 발생하면, 네트워크 노드는 입력 트래픽이 악의적이다 라고 판단하는 것이 아니라 이상 트래픽이다 라고 주로 판단할 것이다 만일 모든 이상 트래픽이 악의적인 공격에 의한 트래픽 이었다면 이상 트래픽을 서비스 하는 것은 의미가 없다. 이상 트래픽을 제어하는 ATC에서 정상 트래픽의 블록킹 확률은 이상 트래픽을 차단하는 ATC에서 보다 더 높게 된다. 그러므로, 글로벌 네트워크에서는 2가지 요인이 고려되어야 한다: 먼저, 총 도착 트래픽 대비 이상 트래픽의 비율; 그리고 두번째로 이상 트래픽 대비 유효 트래픽의 비율이다

Q_{at}를 총 도착 트래픽 대비 이상 트래픽의 비율로, 그리고 Q_{ea}를 이상 트래픽 대비 유효 트래픽의 비율로 정의하자. Q_{at}과 Q_{ea}값 자체를 계산하는 것은 본 논문의 범위를 벗어나는 것이다 아래에서는 제안된 ATC 방식을 Q_{at}과 Q_{ea}값들이 주어지는 경우에 대해서 분석하며, 이를 통해 기존 방식 대비 ATC 방식의 효과에 대해 소개하고자 한다 이상 트래픽 세션의 상호 도착시간과 서비스시간은 각각 평균이 $1/\zeta$과 $1/\nu$인 지수분포를 따른다고 가정한다

IV. 성능측정인자들

1 이상 트래픽이 없는 환경에서 기존 네트워크를 위한 Erlang Loss 모델

악의적인 공격이 없는 랜덤 에러 발생 환경에서, 성능가용성(performability)은 성능 모델과 가용성 모델로 구성된다 참고문헌 [7]에 의하면, 조합된 성능과 가용성 분석을 위한 혼합 모델과 상태 다이어그램이 소개되어 있다. 계층적인 접근방법을 소개하고 있으며, 이 접근방법에서 그림 3에서 보는 바와 같이 상위 레벨 가용성 모델은 마코브 재생 모델 (MRM)로 되는데, 여기서 재생율은 그림 4에서 보듯이 성능 모델로부터 계산되며 그 값은 상위 가용성 모델에 제공되게 된다

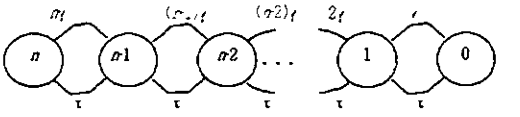


그림 3 Erlang loss 가용성 모델의 상태 다이어그램

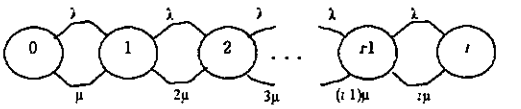


그림 4 Erlang loss 성능 모델의 상태 다이어그램

먼저 가용성 모델은 채널의 실패 복구 행위를 고려하기 위해 소개되며, 그리고 성능 모델은 실패하지 않은 채널의 수가 주어지는 경우 세션 블록킹 확률과 같은 성능 인자를 계산하기 위해 사용되고; 마지막으로 2가지 모델은 함께 조합되어 관심이 있는 성능가용성 측정인자를 제공하게 된다 이때, 가용성 모델은 그림 3에서 보듯이 상태 다이어그램을 가지는 동차의 연속시간 마코브 체인 (CTMC) 이 된다 여기서, 상

태 인자는 시스템에서 실패하지 않은 채널의 수를 나타낸다 시스템에서 실패하지 않은 채널 수 i 를 위한 정상상태 확률 π_i는 다음과 같이 주어진다

$$\pi_i = \frac{1}{i!}(\tau/\gamma)^i \pi_0 \qquad i=1,2,\ \ ,n \tag{4 1}$$

여기서 정상상태 시스템 비가용성은 아래의 수식에 의해 도출된다

$$U = \pi_0 = \left[\sum_{i=0}^{n} \frac{1}{i!}(\tau/\gamma)^i\right]^{-1} \tag{4 2}$$

실패하지 않은 채널 수 i 가 주어지는 경우의 성능 모델을 고려해 보자 관심이 있는 부분은 블록킹 확률, 즉, 모든 버퍼가 사용중인 정상상태 확률인데, 이 경우에 도착 세션은 서비스 거부를 받게 된다. 이 성능 모델에서는 블록킹된 세션은 소실된다 (재시도를 하지 않는다) 라고 가정한다. ATC 시스템의 성능 모델은 *M/M/i* loss 시스템이고 상태 다이어그램은 그림 4와 같다 시스템에 i 채널이 사용될 때의 블록킹 확률은 다음과 같다

$$P_b(i) = \frac{(\lambda/\mu)^i/i!}{\sum_{j=0}^{i}(\lambda/\mu)^j/j!} \tag{4 3}$$

시스템에 i 채널이 사용될 때의 블록킹 확률로서 가용성 모델의 상태 i에 재생율 r_i가 제공된다, 즉, $r_i = P_b(i),\ i \geq 1$ 그리고 $r_0 = 1$이다 이때, 요구되는 총 블록킹 확률은 정상 상태에서의 기대되는 재생율로서 계산될 수 있는데, 다음과 같이 주어진다.

$$T_b = \sum_{i=0}^{n} r_i \pi_i = \pi_0 + P_b(n)\pi_n + \left[\sum_{i=1}^{n-1} P_b(i)\pi_i\right] \tag{4 4}$$

여기서 π_i는 i 개의 실패하지 않은 채널들이 시스템에 있는 경우의 정상상태 확률이다. 총 손실 확률은 3가지 부분으로 구성된다고 볼 수 있다 첫번째 부분은 시스템 비가용성 U이고, 두번째 부분은 시스템내 모든 채널이 사용되고 있는 확률을 가중치로 곱한 버퍼풀 확률에 의한 세션 블록킹 확률이며, 마지막 부분은 열화된 상태의 확률을 가중치로 곱한 열화된 상태 각각에서의 버퍼풀 확률이다

2 이상 트래픽이 있는 환경에서 기존 네트워크 노드를 위한 Erlang Loss 모델

악의적인 공격에 의한 버스트 에러 환경에서 성능 가용성은 성능 모델과 이상 트래픽 모델로 구성된다. 이상 트래픽의 영향은 채널 실패와 복구의 영향보다 훨씬 더 크다 그래서, 실패와 복구의 가용성 모델은 이상 트래픽 모델에 의해 대치될 수 있다. 인터넷상에서 이상 트래픽은 악의적인 공격의 결과로 일어날 수 있는데, 이상 트래픽은 버퍼를 사용하기 때문 네트워크 노드에서 이상 트래픽의 영향은 가용성 모델과 유사하다. 이상 트래픽을 서비스하기 위해 일부 자원이 할당됨으로 해서 시스템 자원이 소비된다 그래서, 정상 트래픽을 위한 가용한 자원은 줄게 된다. 이상 트래픽 모델을 포함하기 위해, 그림 3에서 가용성 모델은 그림 5와 같이 수정될 수 있다. 만일 악의적인 공격이 없다면, 그때 이 모델은 앞서의 이상 트래픽이 없는 네트워크 노드를 위한 Erlang loss 모델과 동일하게 된다

자원 풀에 제한된 수의 자원 (또는 서버) n을 가진 네트워크 노드를 고려한다 계층적인 분해를 통해 근사적인 해결책을 얻을 수 있는데, 우선 가능한 자원의 소유와 해제를 고려하는 상위 이상 트래픽(AT) 모델을 소개하고, 하위 성능 모델이 함께 조합되어 관심이 있는 성능가용성 측정인자를 도출한다

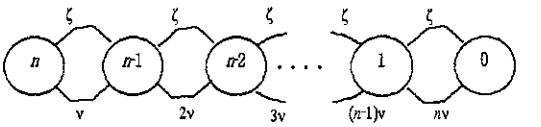


그림 5 Erlang loss 이상 트래픽 모델의 상태 다이어그램

그림 5에서 보여지는 바와 같이 시스템 자원의 소유와 해제를 설명하고 있는 상위 AT 모델은 이상 트래픽 모델이다 Ψ_i(i ∈ {0, 1, 2, ···, n}) 는 상위 이상 트래픽 모델의 상태 i에서의 CTMC의 정상상태 확률이라고 하자. 이 때,

$$\Psi_i = i!\,(\nu/\zeta)^i \Psi_0 \qquad i=1,2,\ldots,n \tag{4 5}$$

여기서 이상 트래픽에 의해 야기되는 정상상태 시스템 비가용성은 다음과 같다.

$$U = \Psi_0 = \left[\sum_{i=0}^{n} i!\,(\nu/\zeta)^i\right]^{-1} \tag{4 6}$$

실패하지 않은 채널의 수가 i인 경우의 성능 모델을 고려한다. 관심이 있는 부분은 블록킹 확률인데, 즉, 모든 버퍼가 사용중인 정상상태 확률을 의미한다 이 경우에 도착하는 세션들은 서비스를 거부 받게 된다. 이 시스템의 성능 모델은 *M/M/i* 손실 모델이고 상태 다이어그램은 그림 4와 같다 이 모델에서 시스템에 i 채널을 사용하는 경우 블록킹 확률은 식(4.3)과 같다. 시스템에 i 채널을 사용하는 경우의 블록킹 확률로서 가용성 모델의 상태 i에 재생율 r_i를 제공

한다, 즉 $r_i = P_b(i), i \gg 1$ 그리고 $r_0 = 1$이다. 이때, 이상 트래픽 조건에서 요구되는 총 블록킹 확률은 정상상태에서의 재생율로서 계산될 수 있는데, 다음과 같다

$$Y_b = \sum_{i=0}^{n} r_i \phi_i = \phi_0 + P_b(n)\phi_n + \left[\sum_{i=1}^{n-1} P_b(i)\phi_i\right] \qquad (4.7)$$

여기서 ϕ_i는 이상 트래픽 조건에서 정상상태 확률인데, i개의 실패하지 않은 채널이 시스템에 있다고 본다 상기에서 총 손실 확률은 3가지 부분으로 구성된다 첫째 부분은 이상 트래픽에 의해 발생하는 시스템 비가용성 U이고, 두번째 부분은 시스템의 모든 채널이 사용되는 확률을 가중치로 곱한 버퍼풀에 기인하는 세션 블록킹 확률이며, 마지막 부분은 이상 트래픽 환경에서 열화된 상태의 확률을 가중치로 곱한 열화된 상태 각각에서의 버퍼풀 확률이다

3 이상 트래픽 제어를 수행하는 ATC를 위한 Erlang Loss 모델

앞 절에 있는 Erlang loss 공식은 이상 트래픽 제어기능을 가진 ATC에 그대로 적용될 수 없는데, 본 장에서는 이상 트래픽 제어 기능을 가진 ATC를 위해 2단계 계층적인 성능가용성 모델을 제안한다

악의적인 공격에 의한 버스트 에러 환경에서 성능 가용성은 성능 모델, 가용성 모델 및 이상 트래픽 제어 모델로 구성된다 이때, 조합되는 ATC와 성능 모델의 혼합모델은 그림 6과 같다. 인터넷에서 이상 트래픽은 악의적인 공격의 결과로 발생할 수 있다. ATC에서의 이상 트래픽 제어의 효과는 가용성 모델보다는 오히려 성능 모델과 유사하다고 할 수 있다 왜냐하면 이상 트래픽의 일부는 정상 트래픽으로 생존하기 때문인데, 이상 트래픽을 서비스 하기 위해 자원의 일부를 할당함으로써 시스템 자원이 소비된다. 그래서, 정상 트래픽을 위한 가용한 자원은 줄게 된다. 이상 트래픽 모델을 포함하기 위해, 그림 4의 성능 모델은 그림 6과 같이 수정되게 되며, 여기서, 예약방식, 즉, 정상 트래픽에 우선순위를 주는 방식이 사용된다.

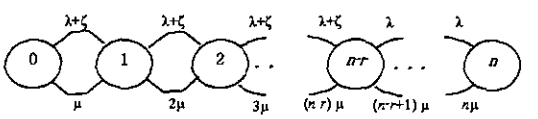


그림 6 Erlang loss 혼합모델을 위한 상태 다이어그램 (정상 + 이상 트래픽)

여기서 r 은 예약된 채널의 수이고 n 은 총 채널 수이다. 분석의 간략화를 위해, 정상과 이상 트래픽의 서비스율은 동일하다고 가정한다. 실패하지 않은 채널의 수가 i 개로 주어지는 경우의 성능 모델을 고려하자 관심이 있는 부분은 블록킹 확률인데, 즉, 모든 버퍼가 사용 중인 정상상태 확률이다. 이 경우에 도착 세션은 서비스가 거부된다 이 성능 모델에서 차단되는 세션은 소실되는 것으로(재시도는 없음) 가정한다. 이 시스템의 성능 모델은 *M/M/i* loss 모델이고 상태 다이어그램은 그림 6과 같다. ATC 기능을 가진 시스템에서 i 채널이 사용되는 경우의 블록킹 확률은 다음과 같다

$$S_b(i) = \frac{((\lambda+\zeta)/\mu)^i / i!}{\sum_{j=0}^{i}((\lambda+\zeta)/\mu)^j / j!}, \quad i = 0,1,2,\ldots,n-r \qquad (4.8a)$$

$$S_b(i) = \frac{((\lambda+\zeta)/\mu)^{n-r}(\lambda/\mu)^{i-n+r}/i!}{\sum_{j=0}^{n-r}((\lambda+\zeta)/\mu)^j/j! + \sum_{j=n-r+1}^{i}((\lambda+\zeta)/\mu)^{n-r}(\lambda/\mu)^{j-n+r}/j!}, \quad i = n-r+1,\ldots,n \qquad (4.8b)$$

이 모델에서 시스템내 실패하지 않은 채널의 수가 i인 경우를 위한 정상상태 확률 π_i은 식 (4.1)과 같다. 시스템내에 i 채널이 사용되는 경우의 블록킹확률로서 가용성모델의 상태 i에 재생율 r_i를 제공하면, 즉, $r_i = S_b(i), i \geq 1$ 그리고 $r_0 = 1$이다. 이때, 정상 트래픽의 요구되는 총 블록킹 확률 W_{rb}는 정상상태에서의 기대되는 재생율로서 계산될 수 있는데, 다음과 같다.

$$W_{rb} = \sum_{i=0}^{n} r_i \pi_i = \pi_0 + S_b(n)\pi_n + \left[\sum_{i=1}^{n-1} S_b(i)\pi_i\right] \qquad (4.9)$$

정상 트래픽의 총 손실 확률은 3가지 부분으로 이루어진다 첫 번째 부분은 실패 복구에 의한 시스템 비가용성 U이고, 두번째 부분은 시스템의 모든 채널이 사용되는 확률을 가중치로 곱한 버퍼풀에 기인하는 세션 블록킹 확률인데, 여기서 버퍼는 정상과 이상 트래픽 모두에 의해 사용되며, 마지막 부분은 열화된 상태의 확률을 가중치로 곱한 열화된 상태 각각에서의 버퍼풀 확률이다

이상 트래픽의 요구되는 총 블록킹확률 W_{ab}은 정상상태에서 기대되는 재생율로서 계산될 수 있는데, 다음과 같다.

$$W_{ab} = \sum_{i=0}^{n-r} r_i\pi_i + \sum_{i=n-r+1}^{n} r_i \sum_{i=n-r+1}^{n} \pi_i = \pi_0 + S_b(n-r)\pi_{n-r} + \left[\sum_{i=1}^{n-r-1} S_b(i)\pi_i + \sum_{i=n-r+1}^{n} S_b(i) \sum_{i=n-r+1}^{n} \pi_i \right] \quad (4\ 10)$$

이상 트래픽의 총 손실확률은 3가지 부분으로 이루어진다 첫번째 부분은 실패 복구에 의한 시스템 비가용성 U이고, 두번째 부분은 시스템의 모든 채널이 사용되는 확률을 가중치로 곱한 $(n\text{-}r)$ 버퍼풀에 기인하는 세션 블록킹 확률인데, 여기서 버퍼는 정상과 이상 트래픽 모두에 의해 사용된며, 마지막 부분은 이상 트래픽을 위해 가용한 최대 $(n\text{-}r)$ 버퍼하에서 열화된 상태의 확률을 가중치로 곱한 열화된 상태의 버퍼풀 확률의 합이다

만일 ATC가 모든 이상 트래픽을 차단 한다면, 이때 정상 트래픽의 요구되는 총 블록킹 확률은 식 (4.4)와 같다 그러나, 이상 트래픽에 관한 차단 정책에 따른 유효 전송율은 이상 트래픽에 대한 제어 정책의 그것과 비교에서 감소하게 된다.

4 유효 트래픽 전송율

성능 모델에서 유효 트래픽 전송율은 중요한데, 여기서는 이상 트래픽을 제어하고 차단하는 정책간에 유효 트래픽의 전송율을 도출하고자 한다 제어 정책을 가지는 ATC에서 유효 신규 세션 시도 λ_{ec}는 다음과 같다.

$$\lambda_{ec} = \lambda + \zeta Q_{ea} \quad (4\ 11)$$

이때, 차단 정책을 가지는 ATC에서 유효 신규 세션 시도 λ_{eb}는 다음과 같다

$$\lambda_{eb} = \lambda \quad (4\ 12)$$

동일한 도착율에서, 이상 트래픽을 차단하는 ATC의 유효 트래픽은 이상 트래픽을 제어하는 ATC의 그것보다 작게 된다 물론, 요구되는 블록킹 확률은 역전이 된다. 이상 트래픽에 대한 제어와 차단간의 유효 전송율의 비 E_{bc} 는 다음과 같다.

$$E_{bc} = \frac{\lambda_{eb}}{\lambda_{ec}} = \frac{\lambda}{\lambda + \zeta Q_{ea}} \quad (4.13)$$

V. 수치계산 결과

본 장에서는 ATC를 위한 수치적인 계산 결과를 보여준다 성능 측정인자로서, 요구되는 세션 블록킹 확률이 이상 트래픽 환경에서의 기존 네트워크 노드와 이상 트래픽을 제어하는 ATC 각각에 대해 도출된다

가정들은 다음과 같다. 평균 신규 세션 시도율 λ =0.1~1.0 세션/초, 평균 세션지속시간 $1/\mu$ =100 초/세션; 채널 수 n = 20, 예약 채널 수 r = 2; 세션지속시간은 지수분포를 따른다; 총 도착 트래픽 대비 이상 트래픽의 비 Q_{at} = 0.3; 그리고 이상 트래픽 대비 유효 트래픽의 비 Q_{ea} = 0 8, 채널 실패와 복구 시간은 각각 $1/\gamma$ = 10,000 그리고 $1/\tau = 1/\mu$, 상호도착시간과 서비스시간 $1/\zeta$와 $1/\nu$는 각각 정상 트래픽 세션의 그것과 동일하다. Mathematica V4.2 패키지가 수치적 계산을 위해 사용되었다 [8].

그림 7은 이상 트래픽 환경에서 정상 트래픽의 도착 빈도가 증가할 때 기존 네트워크 노드에서 요구되는 세션 블록킹 확률을 보여준다 여기서, 총 도착 트래픽 대비 이상 트래픽의 비인 Q_{at}는 0 1 ~ 0 6 구간이다 Q_{at}가 증가될 때, 정상 트래픽의 도착빈도에 비례해서 증가하게 된다. 예를 들어, 정상 트래픽의 도착빈도가 0 15이면, Q_{at}가 0.1, 0 3 및 0 6일때 세션 블록킹 확률은 각각 0.047, 0.051 및 0.758가 된다

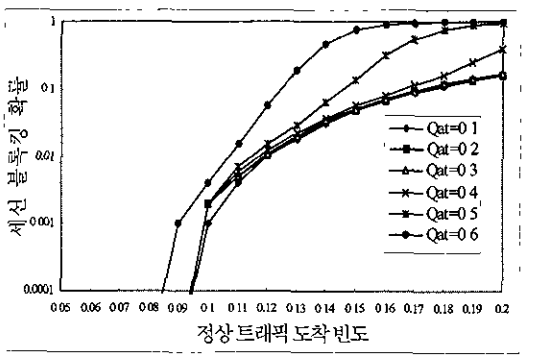


그림 7 도착 빈도가 증가할 때 기존 네트워크 노드에서 요구되는 세션 블록킹 확률

그림 8은 이상 트래픽 환경에서 정상 트래픽의 도착빈도가 증가할 때, ATC의 요구되는 세션 블록킹 확률을 보여준다 여기서, 총 도착 트래픽 대비 이상 트래픽의 비 Q_{at}는 0 1 ~ 0 6 구간이다. Q_{at}가 증가할 때, 블록킹 확률은 정상 트래픽의 도착 빈도에 비례해서 증가하게 된다 그러나, 서로 다른 Q_{at}에서 블록킹 확률간의 차이점은 기존 네트워크 노드와 비교해서 상당히 줄어들게 된다. 예를 들어, 정상 트래픽의 도착 빈도가 0 15이면, Q_{at}가 0.1, 0.3 및 0 6일

때 세션 블록킹 확률은 각각 0 07, 0.107 및 0 150이다.

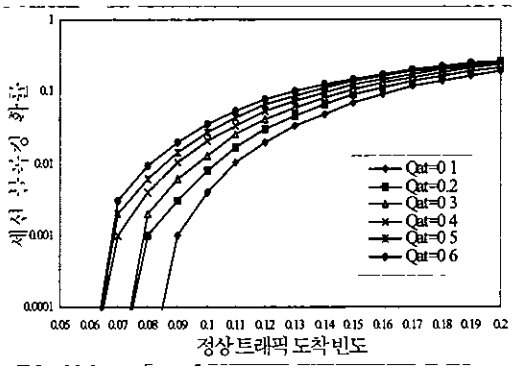


그림 8 도착 빈도가 증가할 때 ATC의 요구되는 세션 블록킹 확률

그림 9는 이상 트래픽 환경에서 예약 채널을 사용하는 경우에 ATC의 요구되는 세션 블록킹 확률을 보여준다. 여기서 가정들은 상기와 같다. 다만 예약 채널의 수 r = 2, 3, 4, 5 및 6이다 r 이 증가할 때 블록킹 확률은 정상 트래픽의 도착 빈도에 반비례로 감소하게 된다. 예를 들어, 정상 트래픽의 도착 빈도가 0 15인 경우, r 이 2, 4 및 6일때 블록킹 확률은 각각 0 107, 0 077 및 0 062이다.

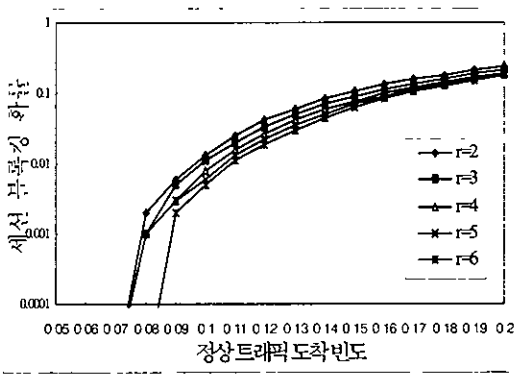


그림 9 예약 채널의 수가 2, 3, 4, 5 및 6인 경우 ATC의 요구되는 세션 블록킹 확률

그림 10은 이상 트래픽에 대해 차단정책과 제어정책을 가지는 ATC의 유효 트래픽 전송율의 비교 결과를 보여준다 Q_{ca}가 증가할 때, 유효 트래픽 전송율은 정상 트래픽에 비례해서 증가하게 된다. 예를 들어, 정상 트래픽의 도착 빈도가 0.15인 경우, 차단정책과 Q_{ca}가 0 3과 0.5일때 제어정책에서 유효 트래픽 전송율은 각각 0 142, 0 166 및 0 189이다

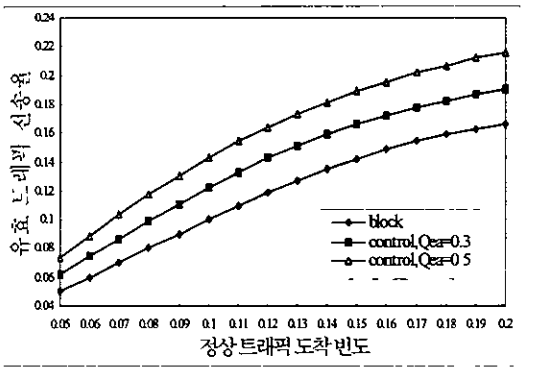


그림 10 차단정책과 Q_{ca}가 0 3과 0 5일때 제어정책에서 유효 트래픽 전송율

그림 11은 이상 트래픽에 대한 차단정책과 제어정책을 가지는 ATC의 유효 트래픽 전송율의 비교결과를 보여준다. 여기서 가정들은 상기와 동일하다 다만, Q_{ca}는 0 1 ~ 0 8 구간이다. Q_{ca}가 증가할 때, 유효 트래픽 전송율은 정상 트래픽에 비례해서 증가한다. 예를 들어, 정상 트래픽의 도착 빈도가 0 15인 경우, 차단정책과 Q_{at}가 0.1, 0.3, 0 5 및 0.8 일때 제어정책에서 유효 트래픽 전송율은 각각 0 142, 0.138, 0 146, 0 154 및 0.166이다. 만일 Q_{ca}가 0 3보다 커다면, 제어 정책을 가지는 ATC가 차단정책을 가지는 ATC보다 우수하다 그 외는 차단정책을 가지는 ATC가 더 우수하다.

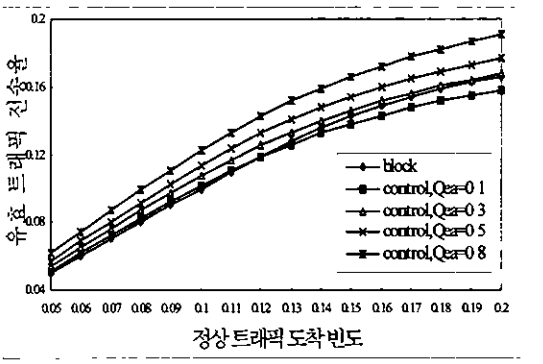


그림 11 차단정책과 Q_{ca}가 0 1, 0 3, 0 5 및 0 8 일때 제어정책에서 유효 트래픽 전송율

VI. 결 론

본 논문에서는 네트워크의 생존성을 보장하고 신뢰성 높은 인터넷 서비스를 제공하기 위한 차세대 보안 기술로서 인터넷의 액세스점에 위치하는 이상 트래픽 제어기를 제안하였다. 네트워크에서 에러의 요인이 계속 존재하거나 반복되는 경우 이상 트래픽 제어를 통해 서비스 완료성을 가능한 보장할 수 있는데, 수치계산 결과에서 보여준 바와 같이 블록킹 확률과 유효 트래픽 전송율 측면에서 이상 트래픽에 대해 제어정책을 가지는 ATC는 기존 네트워크 노드 뿐만 아니라 차단정책을 가지는 ATC 보다 우위에 있다.

미래에는 ATC와 같은 네트워크 공격 대응 기술이 네트워크의 에지나 액세스점에 점차 적용될 것이다. 사용자들은 그들의 시스템에 모든 보안기능을 가질 수 없고, 또한 ISP는 e-service를 제공하는 인터넷 인프라에서 SLA와 같은 품질 보장을 사용자에게 제공해야 할 것이기 때문이다. 향후 연구과제로는 보다 더 현실적인 트래픽 모델이 되기 위해서 트래픽을 몇 가지로 구분, 가령, 프리미엄 정상 트래픽, 정상 트래픽, 프리미엄 이상 트래픽 및 이상 트래픽 등으로 구분하여 모델링 하고 이에 대한 적절한 대응 정책의 연구가 필요하다. 또한, 본 고에서 가정한 이상 트래픽 중 유효 트래픽의 비율을 높이는 탐지기술에 대한 연구가 더 진행되어야 할 것이다.

참 고 문 헌

[1] J.Pescatrore, M. Easley, R.Stiennon, "Network security platform will transform security markets," Gartner, Nov. 2002.

[2] "State of the NGN : Carriers and vendors must take security seriously," Gartner, March 2003.

[3] DARPA FTN, http://www.iaands.org/iaands2002 /ftn/index.html.

[4] Arbor Inc., peakflow, http://www.arbornetworks.com/products_platform.php.

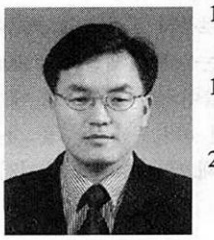
[5] Vern Paxson, Sally Floyd, "Wide area traffic: The failure of poisson modeling," *IEEE/ACM Transaction on networking*, 3(3), pp.226 244, June 1995.

[6] K. S. Kim, M. H. Cho and T. Y. Nam, "Analysis of Session Admission Control based on Area (SACA) for Software Download in Cellular CDMA Systems," ICOIN'2003 Feb. 2003.

[7] Kishor S. Trivedi, Xiaomin Ma and S. Dharmaraja, "Performability modeling of wireless communication systems," Int. Journal of communication systems, pp.561 577 May 2003.

[8] Wolfram Inc., Mathematica V4.2, http://www.wolfram.com.

김 광 식(Kwang-sik Kim) 정회원



1991년 2월 : 경북대학교 전자공학과 졸업

1997년 2월 : 충북대학교 정보통신공학과 석사

2000년 2월 : 충북대학교 정보통신공학과 박사

1991년 1월~2000년 6월 : 한국전자통신연구원 무선방송연구소 선임연구원

2000년 11월~2002년 2월 : (주)투니텔 연구소장

2002년 3월~현재 : 한국전자통신연구원 정보보호연구단 선임연구원

<주관심 분야> CDMA 이동통신, 네트워크보안