네트워크 서비스의 생존성을 높이기 위한 예측기반 이상 트래픽 제어 방식 분석

정회원 김 광 식*

Analysis of abnormal traffic controller based on prediction to improve network service survivability

Kwang sik Kim* ***Regular Member***

요 약

본 논문에서는 네트워크의 생존성을 보장하고 신뢰성 높은 인터넷 서비스를 제공하기 위해 인터넷의 액세스점에 위치하는 예측기반 이상 트래픽 제어기(ATCoP, Abnormal Traffic Controller based on Prediction)를 제안한다. ATCoP는 네트워크로 유입되는 트래픽 중 이상 트래픽을 제어하는 방법으로서, 알려지지 않은 공격에 의해 트래픽이 과다하게 발생하는 경우에, 정상 트래픽에 우선권을 주기 위해 서비스 성공률을 측정하고 그 결과를 기준으로 정상 트래픽용 예약 채널의 수를 결정하여 정상 트래픽의 서비스 수준을 보장함으로써 서비스 생존성을 높히는 방법이다. 만일 예약 채널의 수가 증가하면, 이상트래픽에 할당되는 채널의 수가 감소하게 되어 이상트래픽의 서비스 생존율은 감소하게 된다. 분석결과, 제안 방식은 입력트래픽의 특정 범위에서는 정상트래픽의 블록킹율을 일정 수준으로 유지시켜주는 효과가 있음을 알 수 있었다.

Key Words : Abnormal traffic controller, service survivability, Internet access point, traffic monitoring

ABSTRACT

ATCoP(Abnormal traffic controller based on prediction) is presented to securely support reliable Internet service and to guarantee network survivability, which is deployed in Internet access point. ATCoP is a method to control abnormal traffic that is entering into the network. When unknown attack generates excessive traffic, service survivability is guaranteed by giving the priority to normal traffic than abnormal traffic, that is reserving some channels for normal traffic. If the reserved channel number increases, abnormal traffic has lower quality service by ATCoP system and then its service survivability becomes worse. As an analytic result, the proposed scheme maintains the blocking probability of normal traffic on the predefined level in the specific interval of input traffic.

Ⅰ. 서 론

최근에는 알려지지 않은 공격이 종종 일어나고 있는데, 미래 인터넷 환경에서는 일상적인 것이 될 것이다[1,2]. 알려지지 않은 공격의 경우에 IDS, IPS 및 박스형 보안 어플라이언스와 같은 보안 장비들은 고객망과 접속하는 ISP 인입점의 트래픽에 대하여 오탐지를 할 수 있다. 보안 장비는 이상 트래픽을 막을지 아니면 통과시킬 지에 대해 어려움을 가지게 된다. 왜냐하면, 이상 트래픽의 일부는

* 한국전자통신연구원 정보보호연구단(kks63453@etri.re.kr)
논문번호 : KICS2004-11-294, 접수일자 : 2004년 8월 4일

유효 트래픽이기 때문이다. 여기서 유효 트래픽은 오염된 트래픽이 아닌 인터넷 사용자에 의해 발생된 실제 트래픽을 의미한다.

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[1]. 안전한 인터넷 서비스에 대한 대표적인 연구로는 DARPA FTN (Fault tolerant network)[3]과 Arbor Inc.사 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.

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 악의적이라고 판단하는 것이 아니라 이상 트래픽이라고 주로 판단할 것이다. 만일 모든 이상 트래픽이 악의적인 공격에 의한 트래픽이었다면 이상 트래픽을 서비스 하는 것은 의미가 없다. 이상 트래픽을 적절히 제어하므로 써, 차단에 따른 정상트래픽의 소실보다는 더 높은 전송율을 제공하는 보안기술의 개발이 필요하다. 이러한 연구가 일부[9] 시도 되고 있으며, 실제 환경에 적용을 하기 위해서는 다각적인 연구 분석이 필요하며, 이의 일환으로 본 연구는 예약 채널을 입력 트래픽의 양에 따라 적절히 조정하므로 써 트래픽 서비스율을 높이는 방향에 대해 연구를 진행하였다.

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

Ⅱ. 제안 방식

본 고에서 제안하는 예측기반 이상트래픽 제어 방법은 이상 트래픽 중에서 유효 트래픽을 보호하기 위해 이상 트래픽에 대한 소프트 방화벽 기능의 보안 정책을 수행한다. ATCoP는 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 1은 ATCoP 개념도이다. ATCoP 메인부로 유입되는 트래픽들 중 우선 순위가 있는 정상 트래픽에 우선권을 주면서 채널을 할당한다. white list에 등록된 ip 리스트 판단부는 GIB (Global Information Base)[9]로부터 white list로 등록된 사용자의 ip의 정보를 받아서 저장하여 두고, 유입되는 트래픽의 ip와 비교하여 등록된 ip인지를 판단하여 등록된 ip인 경우만 그 정보를 성공률 판단부로 보낸다. 성공률 판단부는 리스트판단부로부터 수신한 트래픽 정보와 ATCoP의 메인부를 통과한 트래픽 중 white list에 등록된 ip의 트래픽을 수신한 정보의 양을 비교하여 등록 ip의 ATCoP 메인부에서의 서비스 성공률을 측정하게 된다. 예약 채널 수 결정부는 White list ip의 서비스 성공률이 일정 범위 이상으로 우수하면 ATCoP 메인부의 예약채널수를 줄여주고, 성공률이 목표치보다 낮으면 예약채널수를 늘려주도록 ATCoP 메인부에 명령을 내리게 되고, ATCoP 메인부는 예약채널수 결정부가 내린 명령에 따라서 예약채널수를 조정하게 된다.

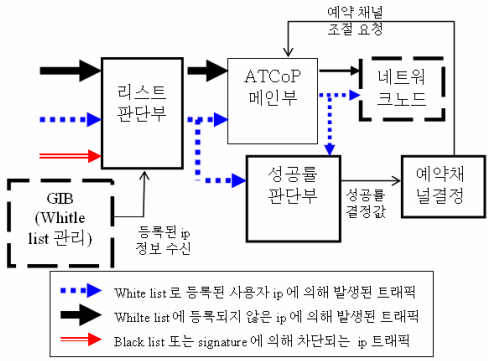

그림 1. ATCoP 개념도.

그림 2는 ATCoP 메인부의 내부 흐름도를 나타낸다. 그림 2에서 패킷 모니터는 패킷의 흐름(flow)의 시작과 끝 시점을 모니터링 한다. ATCoP 메인부에 도착한 패킷은 흐름(flow) 단위로 관리를 받게 되는데, 흐름들은 전화망에서의 채널처럼 가상 채널 연결 단위로 볼 수 있다. 패킷모니터에 유입된 패킷

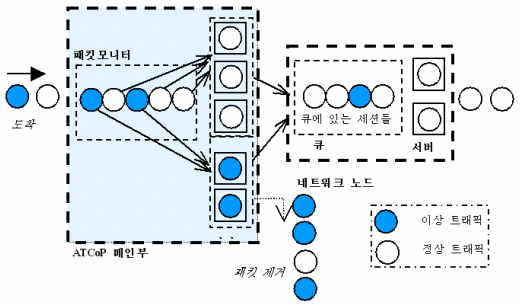

그림 2. ATCoP 메인부의 내부 흐름도

에 대해 패킷모니터는 유입된 패킷에 대해 정상인지 이상한지에 대한 판단을 하게 된다. 만일 패킷이 오염된 패킷으로 의심 된다면 이상 트래픽으로 간주된다.

패킷모니터에서 서버로 전송된 이상 트래픽에 대해 서버는 후 순위를 줌으로써 이상 트래픽을 제어하는데, 제어정책은 차단이나 큐잉을 사용하게 된다. 이상하다고 판단되면 남아있는 채널 중에서 정상 패킷을 위해 예약해둔 채널의 수보다 작으면 손실되고, 예약 채널의 수보다 많이 남아 있으면 서비스 받게 된다. 이와 같이 함으로서, 오염된 패킷은 낮은 생존율을 가지게 되고 전체 유효전송률은 증가하게 될 것이다.

ATCoP는 ADSL 기술을 사용하는 가입자 망에서 DSLAM과 같은 액세스망 노드 근처에 위치할 수 있다. ATCoP는 일종의 전처리 프로세서이며 네트워크 노드에 플러그인 형태나 독립적인 시스템으로 운영될 수 있다. 세션들은 전화망에서의 채널처럼 가상 채널 연결에 의해 서비스 된다고 하자. 그리고 ATCoP는 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 의심된다면 이상 트래픽으로 간주한다. 이상 트래픽에 후 순위를 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

WAN 환경에서 WWW 또는 FTP 세션의 도착 사건은 고정 속도를 가진 포아송 프로세스로 잘 모델링이 된다고 한다[5]. 그리고 세션지속시간은 Pareto 분포를 따른다고 한다. 따라서 본 고에서는 세션지속시간은 지수분포 뿐만 아니라 Pareto 분포를 따르는 것을 고려한다.

3.1 세션의 도착과정

ATCoP는 무한한 세션 요청자가 있다는 가정하에 n 채널을 지원한다고 하자. 세션의 도착은 고정 속도를 가진 동차의 포아송 프로세스의 통계 특성을 근사화 하는 것으로 볼 수 있으며, 아래의 식과 같이 도착 시점간 간격이 속도 파라미터인 λ를 가지는 지수 분포가 된다.

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

이때, ATCoP에서 성공적인 신규 세션 시도는 아래와 같이 주어진다.

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

여기서, P_b는 신규 세션의 블록킹 확률이다.

3.2 세션 크기와 세션지속시간

통계적인 분석이 되기 위해서 세션은 시간축으로 변환되어야 한다. 1Mbits/s의 가상 채널이 사용되고 패킷 헤더, 패킷 ACK 등과 같은 세션의 오버헤드가 50%, 세션당 5개 파일을 가진다고 가정하자. 이때, 표 1은 세션의 지속시간 값을 나타낸다.

표 1. 세션 지속시간

크기구분	파일 크기	세션 크기	세션지속시간
소형	5~100 kbytes	25~500 kbytes	0.4~8 s
중형	100~1,000 kbytes	0.5~5 Mbytes	8~ 80 s
대형	1~5 Mbytes	5~25 Mbytes	80~400 s

세션지속시간은 파라미터 μ를 가지는 독립적 이면서 지수분포를 가지는 랜덤 변수이고, 세션 도착 과정에 독립적이다 라고 가정하면, 세션지속시간 T_s를 지수분포로 고려할 수 있다. 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 서비스율임.

더 현실적으로 말해서, 세션을 구성하는 데이터 파일의 전체적인 통계치는 Pareto 분포에 의해 잘 근사화 된다[9]. 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 m은 분포의 가장 큰 값이고, k는 가장 작은 값이다. α는 분포의 모양을 나타내는 파라미터이다. $(k/m)^{\alpha}$는 Pareto 분포와 차이가 나는 부분으로 조정 값이다.

3.3 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.

3.4 이상 트래픽 반영 인자

여기서는 이상 트래픽을 분석하는데 중요한 2가지 인자, 즉 총 도착 트래픽 대비 이상 트래픽의 비율, 그리고 이상 트래픽 대비 유효 트래픽의 비율에 대해 정의한다.

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 ATCoP 방식을 Q_{at}과 Q_{ea}값들이 주어지는 경우에 대해서 분석하며, 이를 통해 기존 방식 대비 ATCoP 방식의 효과에 대해 소개하고자 한다. 이상 트래픽 세션의 상호 도착시간과 서비스시간은 각각 평균이 $1/\zeta$과 $1/\nu$인 지수분포를 따른다고 가정한다.

Ⅳ. 성능 측정인자들

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

악의적인 공격에 의한 버스트 에러 환경에서 성능가용성은 성능 모델과 이상 트래픽 모델로 구성된다. 참고문헌 [7]에 의하면, 조합된 성능과 가용성 분석을 위한 혼합 모델과 상태 다이어그램이 소개되어 있다. 참고문헌 [7]에서의 접근방법을 사용하여, 조합된 성능과 가용성 분석을 위한 혼합 모델을 도출하며, 그 상태 다이아그램은 그림 3과 4와 같다.

그림 3에서 보는 바와 같이 상위 레벨 가용성 모델은 마코브 재생 모델 (MRM)로 되는데, 여기서 재생율은 그림 4에서 보듯이 성능모델로부터 계산되며 그 값은 상위 가용성 모델에 제공되게 된다.

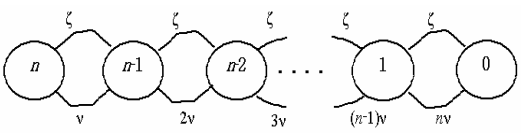

그림 3. Erlang loss 이상 트래픽 모델의 상태 다이어그램.

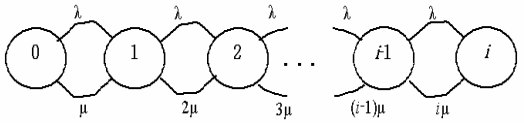

그림 4. Erlang loss 성능 모델의 상태 다이어그램.

인터넷상에서 이상 트래픽은 악의적인 공격의 결과로 일어날 수 있는데, 이상 트래픽은 버퍼를 소비하기 때문에 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.

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 모델을 소개하고, 하위 성능 모델이 함께 조합되어 관심이 있는 성능가용성 측정인자를 도출한다.

그림 3에서 보이는 바와 같이 시스템 자원의 소유와 해제를 설명하고 있는 상위 AT 모델은 이상 트래픽 모델이다. $\Psi_i(i\in\{0, 1, 2, \cdots, n\})$ 는 상위 이상 트래픽 모델의 상태 i에서의 CTMC의 정상상태 확률이라고 하자. 이 때,

$$\Psi_i = i!\,(\nu/\zeta)^i\,\Psi_0, \qquad i=1,2,\ldots,n \quad (4.1)$$

여기서 이상 트래픽에 의해 야기되는 정상 상태 시스템 비가용성은 다음과 같다.

$$U=\Psi_0=\left[\sum_{i=0}^{n} i!\,(\nu/\zeta)^i\right]^{-1} \quad (4.2)$$

실패하지 않은 채널의 수가 i인 경우의 성능 모델을 고려한다. 관심이 있는 부분은 블록킹 확률인

데, 즉, 모든 버퍼가 사용 중인 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 다음과 같다.

$$P_0(i) = \frac{(\lambda/\mu)^i / i!}{\sum_{j=0}^{i} (\lambda/\mu)^j / j!} \qquad (4.3)$$

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 같다.

$$Y_b = \sum_{i=0}^{n} r_i \phi_i = \phi_0 + P_b(n)\phi_n + \left[\sum_{i=1}^{n-1} P_b(i)\phi_i \right] \qquad (4.4)$$

여기서 Ψ_i는 이상 트래픽 조건에서 정상상태 확률인데, i개 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.

4.2 이상 트래픽 제어를 수행하는 ATCoP를 위한 Erlang Loss 모델

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

악의적인 공격에 의한 버스트 에러 환경에서 성능가용성은 성능 모델, 가용성 모델 및 이상 트래픽 제어 모델로 구성된다. 이때, 조합되는 ATCoP와 성능 모델의 혼합모델은 그림 5와 같다. ATCoP에서의 이상 트래픽 제어의 효과는 가용성 모델보다는 오히려 성능 모델과 유사하다고 할 수 있다. 왜냐하면 이상 트래픽의 일부는 정상 트래픽으로 생존하기 때문인데, 이상 트래픽을 서비스하기 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 5와 같이 수정되게 되며, 여기서, 예약방식, 즉, 정상 트래픽에 우선순위를 주는 방식이 사용 된다.

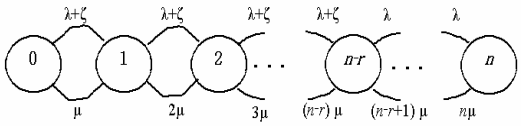

그림 5. Erlang loss 혼합모델을 위한 상태 다이어그램 (정상 + 이상 트래픽).

여기서 r 은 예약된 채널의 수이고 n 은 총 채널 수이다. 분석의 간략화를 위해, 정상과 이상 트래픽의 서비스율은 동일하다고 가정 한다. 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 5와 같다. ATCoP 기능을 가진 시스템에서 i 채널이 사용되는 경우의 블록킹 확률은 다음과 같다.

$$S_b(i) = \frac{((\lambda+\zeta)/\mu)^i / i!}{\sum_{j=0}^{i} ((\lambda+\zeta)/\mu)^j / j!}, \qquad i = 0,1,2,\ldots,n-r \qquad (4.5a)$$

$$S_b(i) = \frac{((\lambda+\zeta)/\mu)^{n-r}(\lambda/\mu)^{i-n+r}/i!}{\sum_{j=0}^{n-r}((\lambda+\zeta)/\mu)^j/j! + \sum_{j=n-r+1}^{i}((\lambda+\zeta)/\mu)^{n-r}(\lambda/\mu)^{j-n+r}/j!}, \quad i = n-r+1,\ldots,n \qquad (4.5b)$$

이 모델에서 시스템내 실패하지 않은 채널의 수가 i인 경우를 위한 정상상태 확률 π_i은 다음과 같다.

$$\pi_i = \frac{1}{i!}(\tau/\gamma)^i \pi_0, \qquad i = 1,2,\ldots,n \qquad (4.6)$$

여기서 정상상태 시스템 비가용성은 아래의 수식에 의해 도출된다.

$$U = \pi_0 = \left[\sum_{i=0}^{n} \frac{1}{i!}(\tau/\gamma)^i \right]^{-1} \qquad (4.7)$$

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_{nb}는 정상상태에서의 기대되는 재생율로서 계산될 수 있는데, 다음과 같다.

$$W_{nb} = \sum_{i=0}^{n} r_i \pi_i = \pi_0 + S_b(n)\pi_n + \left[\sum_{i=1}^{n-1} S_b(i)\pi_i \right] \quad (4.8)$$

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 계산 될 수 있는데, 다음과 같다.

$$\begin{aligned} W_{ab} &= \sum_{i=0}^{n-r-1} r_i \pi_i + r_{n-r} \sum_{i=n-r}^{n} \pi_i \\ &= \pi_0 + S_b(n-r) \sum_{i=n-r}^{n} \pi_i + \sum_{i=1}^{n-r-1} S_b(i)\pi_i \end{aligned} \quad (4.9)$$

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-r*) 버퍼풀에 기인하는 세션 블록킹 확률인데, 여기서 버퍼는 정상과 이상 트래픽 모두에 의해 사용되며, 마지막 부분은 이상 트래픽을 위해 가용한 최대 (*n-r*) 버퍼 하에서 열화된 상태의 확률을 가중치로 곱한 열화된 상태의 버퍼풀 확률의 합이다.

만일 ATCoP가 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 비교해서 감소하게 된다.

4.3 유효 트래픽 전송율

성능 분석 모델에서 유효 트래픽 전송율은 중요하다. 본 장에서는 이상 트래픽을 제어하고 차단하는 정책 간에 유효 트래픽의 전송율을 도출하고자 한다. 동일한 도착율에서, 이상 트래픽을 차단하는 ATCoP의 유효 트래픽은 이상 트래픽을 제어하는 ATCoP의 그것보다 작게 된다. 물론, 요구되는 블록킹 확률은 역전이 된다. 이상 트래픽에 대한 제어와 차단간의 유효 전송율의 비 E_{bc}는 다음과 같다.

$$E_{bc} = \frac{\lambda_{eb}}{\lambda_{ec}} = \frac{\lambda}{\lambda + \zeta Q_{ea}} \quad (4.10)$$

여기서 λ_{ec}는 제어정책을 가지는 ATCoP에서 유효 신규세션 시도, λ_{eb}는 차단 정책을 가지는 ATCoP에서 유효 신규 세션 시도임[9].

4.4 유효 트래픽의 총 블록킹율 계산방법

비정상 트래픽의 차단도 중요하지만 유효 트래픽의 품질 (블록킹 확률)을 유지하는 것이 더 중요하다고 생각되는데, 이를 가능하게 하는 기술이 ATCoP 기술이다. 유효 트래픽의 블록킹 확률 Y_{eb}은 정상 트래픽의 블록킹율과 이상트래픽의 블록킹율, 이상 트래픽 대비 유효 트래픽의 비율 값을 가지고 다음과 같이 구할 수 있다.

$$E_{bc} = \frac{\lambda W_{nb} + \zeta Q_{ea} W_{ab}}{\lambda + \zeta Q_{ea}} \quad (4.11)$$

그림 2의 ATCoP 장치 구성도에서 성공률판단부는 상기 식(4.11)을 이용하여 유효 트래픽의 서비스 성공률을 판단하고 그 값을 예약채널부로 보내면, 예약채널부는 선 정의된 블록킹율과 그 값을 비교하여 초과하면 예약채널수를 증가시키고, 그렇지 않으면 감소시키면서 유효 트래픽의 품질을 일정수준으로 유지하게 한다. 입력되는 트래픽의 일정 수준까지는 예약채널수 조정으로 블록킹율이 일정수준이하로 유지되겠지만, 입력되는 트래픽 양이 많아지게 되면 최대 예약채널수가 n개가 되어도 블록킹율은 일정수준이상을 초과하게 된다. 즉, 제안방식은 특정 입력 트래픽 범위 내에서만 정상적으로 동작하게 된다.

Ⅴ. 수치계산 결과

본 장에서는 ATCoP를 위한 수치적인 계산 결과를 보여준다. 성능 측정인자로서, 요구되는 세션 블록킹 확률이 이상 트래픽 환경에서의 기존 네트워크 노드와 이상 트래픽을 제어하는 ATCoP 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; 예약채널수 r = 2; 세션지

속시간은 지수분포를 따름; 총 도착 트래픽 대비 이상 트래픽의 비 Q_{at} = 0.3, 0.6, 1.0; 그리고 이상 트래픽 대비 유효 트래픽의 비 Q_{ea} = 0.01; 목표 블록킹 확률 Y_{eb} = 1, 2, 5, 10, 20 %; 채널 실패와 복구 시간은 각각 $1/\gamma$ = 10,000 (53분/년) 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].

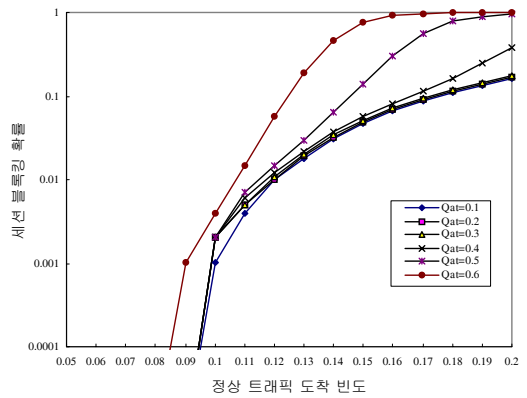

그림 6. 도착 빈도가 증가할 때 기존 네트워크 노드에서 요구되는 세션 블록킹 확률.

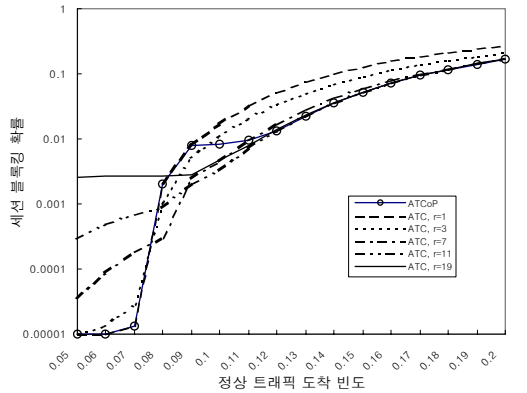

그림 7. 입력트래픽 양의 특정 범위에서 ATCoP의 블록킹율 변화

그림 6은 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 0.758이 된다.

그림 7은 입력트래픽의 증가에 따른 블록킹확률을 보여주고 있다. 그림에서 입력트래픽 양에 상관없이 고정예약채널을 사용하는 기존의 ATC[9]에서는 블록킹율이 보듯이 입력 트래픽 양에 비래해서 증가하게 된다. 그러나 제안 ATCoP에서는 특정 입력 트래픽 범위내에서는 목표 Y_{eb} 값(1%) 이하로 유지됨을 알 수 있다. 이를 위해 예약채널수는 가변하게 된다.

그림 8은 입력트래픽의 증가에 따른 블록킹확률을 보여주고 있다. 여기서, 목표 Y_{eb}값은 1, 2, 5, 10, 20%이다. 목표치에 따라 다른 특성 곡선을 그리게 되는데, 곡선의 형태는 목표치를 기준으로 일정 트래픽 구간에서 완만하다가 곡선을 그리고 있다.

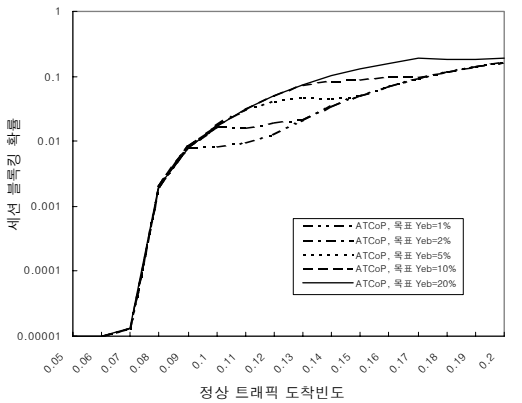

그림 8. 목표로 하는 Y_{eb} 값에 따른 ATCoP의 블록킹율 변화

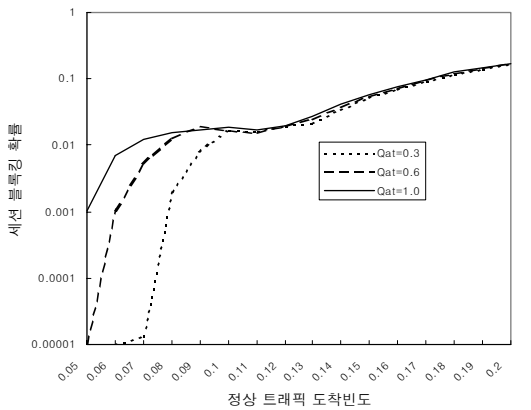

그림 9. Q_{at}값에 따른 ATCoP의 블록킹율 변화 (목표 Y_{eb} =2%)

그림 9는 Q_{at}값에 따른 ATCoP의 블록킹율 변화를 보여준다. 여기서 목표 Y_{eb}=2%이고, Q_{at}값은 0.3, 0.6, 1.0이다. 목표치에 따라 유사한 특성 곡선을 그리지만, Q_{at}값이 클수록 목표 Y_{eb} 값을 가지는 완만한 부분이 더 넓은 것을 알 수 있다. 이는 이상 트래픽이 많을수록 정상트래픽 양이 적은 지점부터 ATCoP의 동작이 시작된다는 것을 알 수 있다.

그림 10은 Q_{ea}값에 따른 ATCoP의 블록킹율 변화를 보여준다. 여기서 목표 Y_{eb}=2%이고, Q_{ea}=1.0, 그리고 Q_{ea}=0.01, 0.05, 0.5이다. Q_{ea} 값이 작을수록 제안 방식이 목표 Y_{eb} 값을 입력트래픽 변화에 따라 일정치를 유지하려는 범위가 넓다. Q_{ea}가 0.05일때는 목표치 유지하려는 입력 트래픽 폭이 좁으며, Q_{ea}=0.5인 경우는 ATCoP가 제대로 동작하지 않음을 알 수 있다.

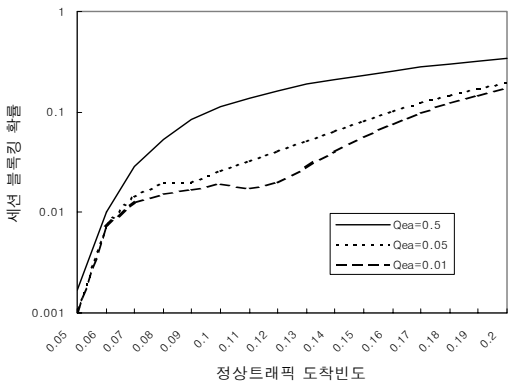

그림 10. Q_{ea}값에 따른 ATCoP의 블록킹율 변화 (목표 Y_{eb}=2%, Q_{at}=1.0)

그림 11은 Q_{ea}값에 따른 ATCoP의 블록킹율 변화를 보여준다. 여기서 목표 Y_{eb} =10%이고, Q_{ea} =1.0, 그리고 Q_{ea}=0.01, 0.05, 0.5이다. 그림 10과는 달리 Q_{ea}가 0.05일때도 Q_{ea}=0.01일때와 비슷하게 목표치를 유지하는 입력 트래픽 폭이 넓다. 즉, 목표치가 낮을수록 ATCoP의 이상트래픽 판단의 정확도가 낮아지더라도 잘 동작함을 알 수 있다. 그러나 Q_{ea}=0.5인 경우에는 그림 10과 같이 여전히 ATCoP가 제대로 동작하지 않음을 알 수 있다.

상기 분석을 통해 다음과 같은 결론을 얻었다. ATCoP의 패킷모니터의 이상트래픽 판단의 정확도가 높을수록 제안 방식은 잘 동작하지만, 5%이상 오탐지율을 가지는 경우는 ATCoP 적용에 따른 효과가 별로 없다는 것을 알 수 있었다. 따라서 이상 트래픽 판단의 정확도를 높이는 연구를 앞으로 계속 진행해야 한다.

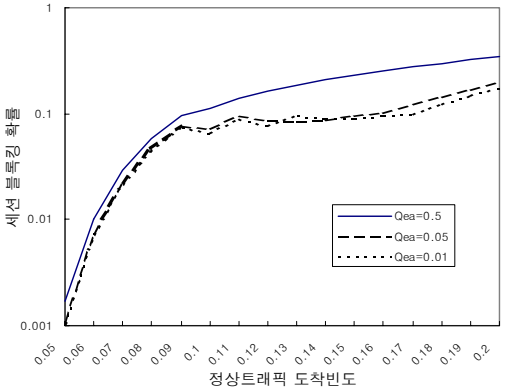

그림 11. Q_{ea}값에 따른 ATCoP의 블록킹율 변화 (목표 Y_{eb}=10%, Q_{at}=1.0)

Ⅵ. 결 론

본 제안방식은 네트워크로 유입되는 이상 트래픽을 적절히 제어하여 네트워크의 생존성을 보장하고 신뢰성 높은 인터넷 서비스를 제공할 수 있다. 네트워크에서 에러의 요인이 계속 존재하거나 반복되는 경우 이상 트래픽 제어를 통해 서비스 완료성을 가능한 보장할 수 있는데, 블록킹 확률과 유효 트래픽 전송율 측면에서 이상 트래픽에 대해 제어정책을 가지는 ATCoP는 기존 네트워크 노드 뿐만 아니라 차단정책을 가지는 ATCoP 보다 우위에 있게 된다. 미래에는 ATCoP와 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.

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/iaands 2002/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.
〔9〕 K. S. Kim, T. Y. Nam, and C. M. Han, "Analysis of Abnormal traffic controller deployed in Internet access point," ICOIN' 2004, Feb. 2004.

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
<관심분야> CDMA 이동통신, 네트워크보안