# 시계열 모델 기반 트래픽 이상 징후 탐지 기법에 관한 연구

정회원 조 강 홍*, 이 도 훈**

# A Study on Traffic Anomaly Detection Scheme Based Time Series Model

Kang Hong Cho*, Do Hoon Lee** *Regular Members*

요 약

본 논문에서는 시계열 예측 모델을 이용하여 웜 또는 바이러스 등과 같은 공격 트래픽에 의해 네트워크상에 발생할 수 있는 트래픽 이상 징후를 탐지할 수 있는 예측 모델 기반 트래픽 이상 징후 탐지 기법을 제안한다. 제안 기법은 비교적 정확한 예측모델로 알려져 있는 ARIMA 모델을 이용하였고 이상 징후 여부를 확률값으로 변화하여 확률 임계값에 따라 이상 징후를 탐지하도록 하여 그 성능을 극대화할 수 있도록 하였다. 이를 위해 제안 기법을 네트워크상에 발생시킨 웜과 같은 비정상 공격 트래픽을 포함한 전체 트래픽과 웹 트래픽에 적용하여 트래픽의 이상 징후를 신뢰성 있는 수준에서 탐지함을 보여주었다. 이 기법을 네트워크 기반의 침입탐지시스템에 적용할 경우에 큰 효과 가져올 수 있을 것이다.

**Key Words :** Anomaly, Time Series, ARIMA, AR, 웜, 바이러스, AR, Anomaly Detection

ABSTRACT

This paper propose the traffic anomaly detection scheme based time series model. We apply ARIMA prediction model to this scheme and transform the value of the abnormal symptom into the probability value to maximize the traffic anomaly symptom detection. For this, we have evaluated the abnormal detection performance for the proposed model using total traffic and web traffic included the attack traffic. We will expect to have an great effect if this scheme is included in some network based intrusion detection system.

## Ⅰ. 서 론

인터넷의 사용자가 크게 증가함에 따라 인터넷 트래픽의 양도 크게 증가하고 있다. 정상적인 인터넷 트래픽의 증가와 더불어 웜, 바이러스, 해킹 등과 관련된 비정상적인 트래픽의 양도 급속히 증가하고 있다. 이와 같은 비정상적인 트래픽은 네트워크에 영향을 미쳐 인터넷의 정상적인 사용을 위협하여 인터넷 속도를 느리게 하거나 최악의 경우 사용할 수 없도록 큰 영향을 끼친다.

이와 같이 늘어나는 인터넷 침해 사고에 능동적으로 대응하기 위해 일반적으로 침입 탐지 시스템을 사용하고 있다. 그러나 기존의 침입 탐지 시스템은 여러 가지 제약사항을 가지고 있다. 먼저, 정해진 규칙과 로그에만 의해 동작하기 때문에 최근에 다양하게 새롭게 발생되는 웜, 바이러스 등에 조기에

※ 본 연구는 동양공업전문대학 학술연구과제의 연구비 지원으로 수행되었습니다.
* 동양공업전문대학 (khcho@dongyang.ac.kr), ** 국가보안기술연구소 (dhlee@ensec.re.kr)
논문번호 : KICS2008-02-065, 접수일자 : 2008년 2월 4일, 최종논문접수일자 : 2008년 5월 23일

대응하는 것이 어렵다. 인터넷 침해 사고가 발생했을 경우 피해를 최소화하기 위해서는 조기에 탐지하여 피해의 확산을 줄이는 것이 굉장히 중요하다. 또한, 기존의 침입 탐지 시스템은 단순화된 모델을 이용하여 정상 트래픽과 비정상 트래픽을 신뢰성 있게 탐지하여 알려주는 성능이 높지 않다. 이와 같은 신뢰성의 문제 때문에 비정상 트래픽에 대한 탐지 오인율이 높기 때문에 이에 대한 연구가 계속적으로 진행되고 있다[8]. 이를 위해서는 조기에 정상 트래픽과 비정상 트래픽을 구분하여 이상 트래픽을 탐지하고 이를 알려주는 이상 징후 탐지 기법이 추가적으로 필요하다.

본 논문에서는 트래픽 이상 징후를 탐지하는 탐지 확률을 높이고 오인율을 최소화하기 위해 시계열 모델 중 비교적 정확한 예측 모델로 알려진 ARIMA(Autoregressive Integration Moving Average) 모델을 이상 징후 탐지를 위해 적용하였다. ARIMA 모델은 예측값에 대한 신뢰 범위를 제공함으로써 해당 데이터에 대한 동적 임계값을 제공할 수 있으며 또한, 이를 근거로 실측 데이터가 이상 상태인지 아닌지를 확률값으로 제공할 수 있는 장점을 가진다. 이 제안하는 기법을 네트워크상에 발생시킨 웜과 같은 비정상 공격 트래픽을 포함한 전체 트래픽과 웹 트래픽에 적용하여 트래픽의 이상 징후를 탐지하는 성능을 평가하도록 하겠다.

## Ⅱ. 관련 연구

본 논문에서는 트래픽 이상 징후를 탐지하기 위해 통계학에서 널리 쓰이고 있고 비교적 정확하다고 알려져 있는 시계열 예측 모델을 적용하였다. 이와 같이 시계열 데이터를 이용하여 트래픽 특성을 분석하고 이상 상태를 구별하기 위한 연구는 다양한 방법을 통해서 진행되어왔다.

이전의 논문들에서는 단순히 시계열 예측 모델을 통해 네트워크의 트래픽을 예측하는 연구들이 많이 이루어졌다. 논문 [1]에서는 시계열 모형을 이용해 장기간의 NSFNET 백본 네트워크의 트래픽을 분석하고 앞으로의 트래픽 증가량을 예측하였고, 논문 [2]에서는 seasonal ARIMA 모델을 이용해 무선 트래픽을 모델링하고 예측하는 연구를 수행하였다. 논문 [3]에서는 네트워크 트래픽 시계열 정보로부터 단순한 임계값을 통한 이상 여부의 판단이 아닌 트래픽 예측 모형의 분석을 통해 트래픽의 특성이 바뀌었는지를 판단하는 동적 임계값 기법을 제시하였으며, 논문 [4]에서는 일정 단위의 네트워크상의 서버에 대한 트래픽 시계열 데이터를 이용해 과도한 트래픽으로 네트워크 안의 파일 서버가 다운될 수 있는지 예측하는 기법을 제시하였다.

최근의 연구는 트래픽의 급속한 증가에 따른 다양한 네트워크 침입 및 공격과 관련된 연구들이 계속적으로 수행되고 있다.

논문 [5]에서는 지수평활법을 이용해 광대역 네트워크에서 발생할 수 있는 실시간 공격을 탐지할 수 있는 네트워크 침입 탐지 기법을 제안하였고, 논문 [6]에서는 웹 서버에 대한 다양한 DDoS 공격을 TCP 헤더 내의 플래그 값을 분석하여 공격 여부를 판단 및 구분하는 트래픽 비율 분석법을 제시하였다. 또한, 논문 [7]에서는 패킷 헤더 정보 대신에 패킷의 수와 트래픽 양의 비율을 구하여 공격 여부를 판단하는 기법을 제시하였다. 논문 [14]에서는 시계열 모형이 네트워크 트래픽 예측에 적합한지를 검증한 내용으로 본 논문과 관련하여 시계열 모델의 신뢰성을 높여줄 수 있다.

앞에서 제시한 다양한 형태의 기법들은 기본적으로 비교적 단순한 계산 모델을 적용하여 정확성이 떨어지며 해당 기법들을 이용해 계산된 결과 값이 네트워크 공격에 따른 정상인지 이상인지를 판단할 수 있는 기준을 제시하지 않았기 때문에 실제 네트워크에 적용하여 사용하는 것이 쉽지 않다.

본 논문에서는 네트워크 트래픽 특성을 비교적 정확히 분석하고 이상 여부를 판단하기 위해 시계열 모델 중 ARIMA 모델을 사용하였고, 공격 및 이상 여부를 확률값에 근거하여 판단할 수 있는 확률 임계값을 제공하여 각 네트워크 환경의 특성에 따라 다르게 적용함으로써 탐지 확률을 높일 수 있도록 하였다.

## Ⅲ. 제안하는 이상 징후 탐지 기법

기본적으로 시계열 예측은 예측될 변수 자체의 과거의 자료에서 어떠한 패턴을 발견하여 미래에도 그러한 패턴이 특성을 잃지 않고 반복될 것이라는 가정 하에 모형을 확립하여 예측하는 방법이다. 그러므로 확립된 시계열 모형은 특정한 자료의 집합에 모형이 얼마나 잘 적합한가에 의하여 전적으로 평가되어진다. 정확한 탐지를 위해서는 각각의 특징을 가지는 네트워크 트래픽에 대한 적절한 예측 모델을 식별하고 결정하는 과정이 필수적이다. 그림 1은 이와 같은 시계열 모델에서 데이터를 적용하여

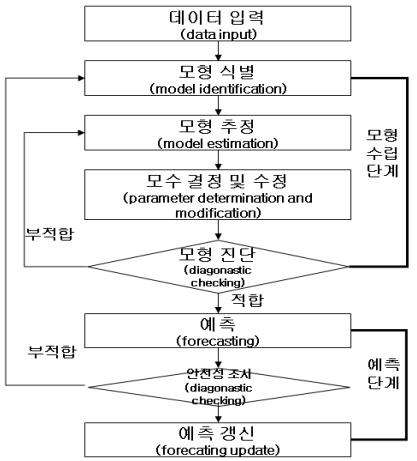


그림 1. 시계열 예측 단계

예측하는 과정을 보여주고 있다. 이 과정에 따라 본 논문에서 제시하는 기법을 설명하고자 한다.

본 논문에서는 수집된 시계열 데이터를 분석하여 그림1의 모형 식별 단계에서 자기상관함수(ACF, AutoCorrelation Function) 및 편자기상관함수(Partial AutoCorrelation Function)를 계산한 결과 가장 적합한 모델로 2차의 자기회귀모형(AR, Autoregressive Model)을 선택하였다[9][10].

AR(Autoregressive) 모형은 계산의 복잡성이 높지 않고 단기 예측에 비교적 정확한 성능을 보이고 있어 이미 네트워크 트래픽 예측에 많이 사용되고 있다[3][11].

AR 모형은 현시점 $t$에서의 시계열 $Z_t$는 $p$개의 과거값들의 가중치 값과 이것들로 설명되지 않은 오차항 $a_t$의 선형결합으로 표현된다.

$$Z_t = \phi_1 Z_{t-1} + \phi_2 Z_{t-2} + \cdots + \phi_p Z_{t-p} + a_t$$
$$= \sum_{j=1}^{p} \phi_j Z_{t-j} + a_t \quad (1)$$

여기서 $a_t$는 $t$시점의 오차로서 평균 0과 분산 $\sigma_a^2$을 가지는 독립이고 동일한 분포의 확률 변수이고, $\phi_j$ 는 자기회기 모형의 모수이다. 이 모형을 통하여 선시차 $l$의 트래픽 예측값을 계산할 수 있다. 시점이 $t$이고 선시차가 $l$인 트래픽 예측값 $\hat{Z}_t(l)$의 최소 평균제곱오차 예측의 일반식은

$$\hat{Z}_t(l) = E\{Z_t(l) \mid Z_t(l), Z_{t-1}(l), \cdots)\} \quad (2)$$

이며, 이 때 $AR(p)$ 모형을 통한 선시차 $l$의 예측식은

$$\hat{Z}_t(l) = \sum_{j=1}^{p} \phi_j Z_t(l-j) \quad (3)$$

이다. 여기서 예측 오차는

$$e_t(l) = Z_t(l) - \hat{Z}_t(l)$$

이므로, 위의 식을 통해 이 예측 오차를 계산하면

$$e_t(l) = \sum_{j=0}^{l-1} \phi_j Z_t(l-j) \quad (4)$$

이다. 예측 오차가 계산되면 미래값에 대한 신뢰구간을 계산할 수 있다. 앞의 AR 모형의 오차항이 정규분포 $N(0, \sigma_e^2)$을 따른다면 역시 예측 오차도 평균이 0이고 분산이 $\sigma^2(l) = \sigma_e^2 \sum_{j=0}^{l-1} \phi_j^2$ 인 정규분포를 따르므로, 신뢰구간은

$$P(-Z_{\frac{\alpha}{2}} < \frac{Z_{t+l} - \hat{Z}_t(l)}{\sqrt{Var(e_t(l))}} < Z_{\frac{\alpha}{2}}) = 1-\alpha \quad (5)$$

이고, 예측값에 대한 $(1-\alpha)100\%$의 신뢰구간은 다음과 같다.

$$\hat{Z}_t(l) \pm Z_{\frac{\alpha}{2}} \sqrt{\sigma_e^2 \sum_{j=0}^{l-1} \phi_j^2} \quad (6)$$

단, $N_{\frac{\alpha}{2}}$는 $P(N > N_{\frac{\alpha}{2}}) = \frac{\alpha}{2}$인 표준정규분포값이다. 이와 같이 계산된 신뢰 구간 중 $upper_t(l)$는 상위 임계값으로 트래픽 이상 징후를 판단하는 임계값으로 사용된다.

$$upper_t(l) = \hat{Z}_t(l) + Z_{\frac{\alpha}{2}} \sqrt{\sigma_e^2 \sum_{j=0}^{l-1} \phi_j^2} \quad (7)$$

트래픽 데이터만을 가지고는 네트워크 상의 트래픽의 변화 정도, 즉 이상 징후를 쉽게 구별하기 어렵기 때문에 실측 데이터의 임계값 위반 정도를 측정하기 위해 식 (8)을 이용해 실측 데이터가 임계값을 넘어가는 정도를 표준정규분포를 통해 정규화하여 0~1사이의 분포값으로 변환한다.

$$S_t(l) = P(\frac{upper_t(l) - Z_t(l)}{\sigma_t(l)}) \quad (8)$$

$$if\,(S_t(l) > Th_\lambda)\,abnormal$$
$$else\ \ normal$$

변환된 $S_t(l)$와 이상 상태 판단하기 위한 탐지 확률 임계값 ($Th_\lambda$ : 확률값이 $\lambda$인 임계값)과 비교하

여 확률 임계값을 넘어가면 이상 징후로 판단한다. t 시점에서 이상 징후 여부를 판단한 후, 계속적인 탐지를 위해 현재 실측된 데이터를 다음 시점인 t+1의 예측값을 갱신하기 위해 식(9)를 적용해서 반복적으로 기법을 적용시킨다. 그런데, 만약 t 시점에서 이상 상태로 판단되었다면 이 때의 트래픽은 정상 상태가 아니므로 다음 시점의 예측값과 임계값의 정확성을 높이기 위해 적용되지 않아야 한다.

$$\hat{Z}_{t+1}(l) = \hat{Z}_t(l+1) + \phi_l(Z_{t+1} - \hat{Z}_t(1)) \quad (9)$$

그림 2는 지금까지 설명한 이상 징후 탐지 기법의 동작 과정을 보여준다.

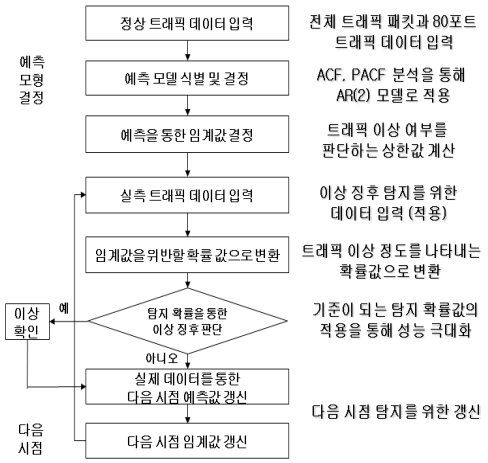


그림 2. 이상 징후 탐지 기법의 동작 과정

## Ⅳ. 실험 및 결과

본 논문에서 제안하는 기법의 성능 평가를 위해 웜 발생기를 이용한 테스트 환경을 구축하고, 정상 상태의 트래픽과 CodeRed, Nimda 등의 웜 공격 트래픽을 혼합하여 발생시켰다. 이를 위해 유니텔 코퍼레이션의 트래픽 발생 및 분석 장비인 SmartBits와 공격 트래픽 및 악성코드 발생 장비인 ThreadEx를 이용했다[11][12]. 2007년 9월 5일부터 9일까지 5일간의 발생시킨 트래픽을 전체 패킷 개수와 CodeRed, Nimda 등의 공격에 사용되는 80번 포트의 패킷 개수를 1분 단위로 수집하였고, 이 때 발생시킨 총 공격 발생 횟수는 95번 이었다.

그림 3은 수집 기간 동안의 전체 트래픽과 80번 포트 트래픽의 일부 시계열 데이터이며, 그림 4는 제안하는 탐지 기법을 이 시계열 데이터에 적용한 결과로 Ⅲ 장의 수식에서 제시한 실제값($Z_t$)과 예측값($\hat{Z}_t(l)$), 그리고 임계값($upper_t(l)$)의 계산 결과를 그래프를 통해 보여주고 있다.

그림 5는 전체 트래픽이 제시하는 임계값을 위반하게 될 확률값으로 변환된 $S_t(l)$ 데이터와 이상 징후를 판단하기 위해 탐지 확률 임계값($Th_\lambda$)을 각각 50%, 60%, 70%, 80%로 적용한 이상 징후 탐지 결과를 보여주는 그림이다. 그림에서 각 확률 임계값을 초과한 경우 이상 징후로 판단하고 탐지하게 된다. 그림 6 과 그림 7은 마찬가지 방법으로 80번

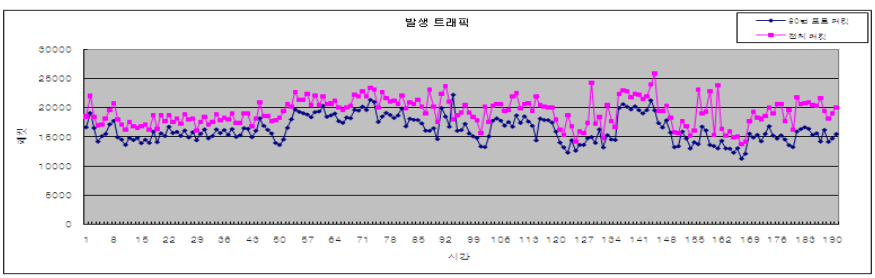


그림 3. 전체 트래픽과 80번 포트 트래픽 시계열 데이터

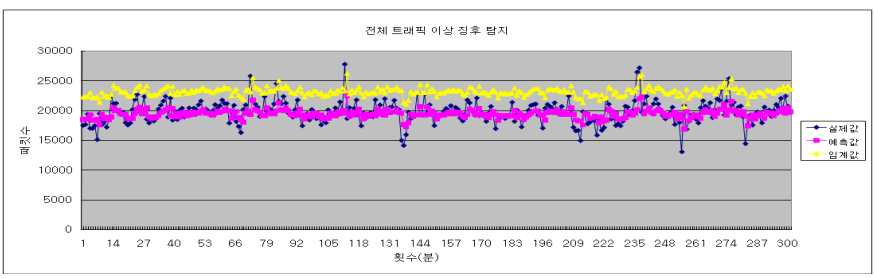


그림 4. 전체 트래픽을 탐지 기법에 적용한 결과

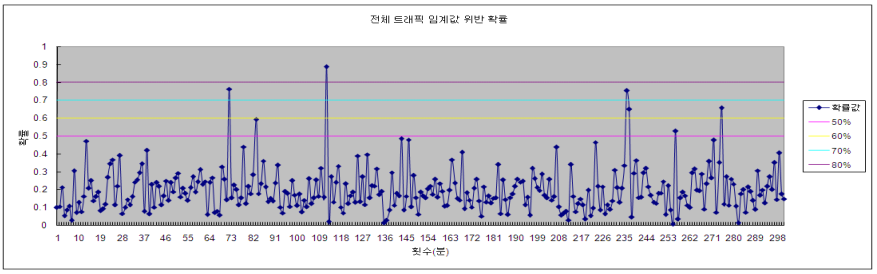


그림 5. 전체 트래픽에 대한 이상 징후 탐지

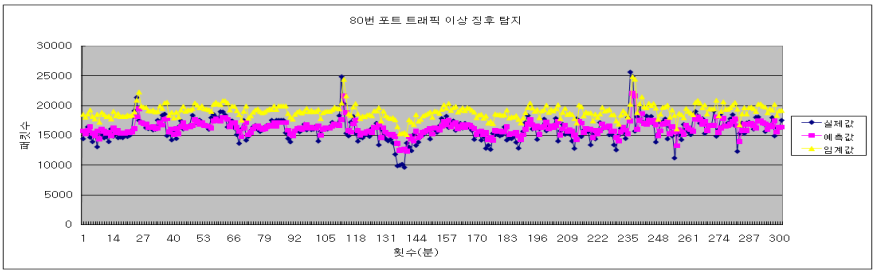


그림 6. 80번 포트 트래픽을 탐지 기법에 적용한 결과

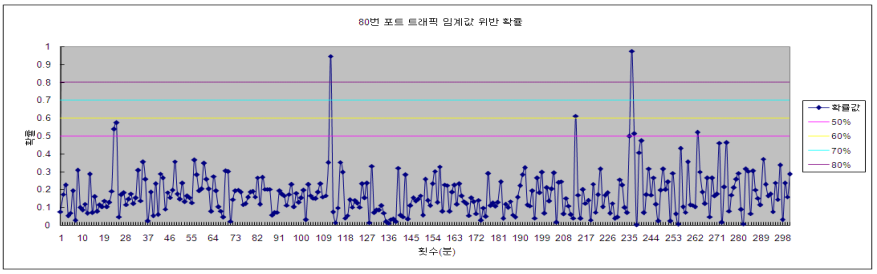


그림 7. 80번 포트 트래픽에 대한 이상 징후 탐지

포트 트래픽에 대한 실험 결과를 보여준다.

그림에서 보는 바와 같이 임계값을 너무 낮게 설정하면 정상 트래픽을 공격 트래픽으로 간주하여 빈번한 탐지 결과를 보여주고, 확률 임계값을 너무 높게 설정하면 실제 발생한 공격에 대해 탐지하지 못하는 오류가 발생된다. 따라서 실험을 통해 적절한 확률 임계값을 찾고 이를 적용하는 것이 높은 탐지 성능을 보이게 된다.

표 1은 실험 기간 동안의 전체 트래픽에 대해 발생시킨 공격을 탐지한 탐지 횟수를 보여준다. 탐지율은 발생시킨 공격을 실제로 탐지한 비율을 나타낸다. 보는바와 같이 탐지확률 임계값($Th_\lambda$)을 60%로 적용했을 경우 성능을 평가하는 탐지율이 가장 높게 나왔으며, 실험에서 웹에 근거한 공격 트래픽을 발생시켰기 때문에 80번 포트 트래픽에 대해 탐지 기법을 적용했을 경우 역시 60% 탐지 확률 임계값에서 가장 좋은 탐지율을 보였다.

표 1. 탐지확률에 따른 탐지 성능 분석

| 탐지확률 | 전체 트래픽 | | | 80포트 트래픽 | | |
|---|---|---|---|---|---|---|
| | 탐지 | 탐지오류 | 탐지율 | 탐지 | 탐지오류 | 탐지율 |
| 50% | 121 | 26 | 72.6% | 116 | 21 | 77.9% |
| 60% | 108 | 13 | 86.3% | 103 | 8 | 91.6% |
| 70% | 77 | 18 | 81.1% | 81 | 14 | 85.3% |
| 80% | 48 | 47 | 50.1% | 58 | 37 | 61.6% |

## V. 결 론

본 논문에서는 시계열 예측 모델을 이용하여 네트워크상에 발생할 수 있는 트래픽 이상 징후를 탐지할

수 있는 예측 모델 기반 트래픽 이상 징후 탐지 기법을 제안하였다.

제안하는 기법을 웜과 바이러스 등의 네트워크 트래픽 공격을 통해 발생된 전체 트래픽과 웹 트래픽에 적용하여 트래픽의 이상 징후를 신뢰성 있는 수준에서 탐지함을 보였다. 또한, 탐지확률을 통해 적용하는 네트워크의 특성에 따라 다르게 나타날 수 있는 이상 징후 탐지의 성능을 향상시킬 수 있도록 적용하였다. 제안하는 기법의 경우 기존의 침입탐지시스템이 가지지 못하는 네트워크상의 트래픽 이상 징후와 새롭게 발생되는 공격의 경우에도 신뢰성 있는 탐지가 가능하기 때문에 이 기법을 기존의 침입탐지시스템에 적용할 경우에 상호보완적으로 큰 성능 향상 효과 가져올 수 있을 것으로 예상된다.

추가적으로 현재 좀 더 정확한 실험 결과를 위해 웹 트래픽의 공격 외에 다른 추가적인 네트워크 공격에 대한 시계열 데이터를 통해 연구 중이며, 실험 결과와 같이 공격에 해당되는 각 포트별 트래픽에 대해 제안하는 기법을 적용할 경우, 좀 더 좋은 성능을 보일 수 있을 것으로 기대된다.

## 참 고 문 헌


〔1〕 Nancy K. Groschwitz, George C. Polyzos, “A Time Series Model of Long-Term NSFNET Backbone Traffic”, ICC’94, pp.1400-1404, 1994

〔2〕 Yantai Shu, Minfang Yu, Jiakun Liu, Yang, O.W.W., “Wireless traffic modeling and prediction using seasonal ARIMA models”, Communications, 2005. IEIEC Transactions on Communications 2005, E88-B, pp.3992-3999

〔3〕 Cynthia S. Hood, Chuanyi Ji “Beyond Thresholds: An Alternative Method for Extracting Information from Network Measurements”, GLOBELCOM’97, pp.487-491, 1997

〔4〕 Cynthia, S. Hood, Chuanyi Ji, “Proactive Network Fault Detection”, INFOCOM’97, pp.1147-1155 vol.3, 1997

〔5〕 권기훈, 한영구, 정석봉, 김세헌, 이수형, 나중찬, “트래픽 분석에 의한 광대역 네트워크 조기 경보 기법”, 정보보호학회논문지, 제14권 제 4호, 2004. 8

〔6〕 강길수, 이준희, 최경희, 정기현, 심재홍, “DDos 공격 탐지를 위한 패킷 샘플링 기법들의 성능 분석”, 정보처리학회논문지 제11-C권, 제6호, 2004. 12

〔7〕 이철호, 최경희, 정기현, 노상욱, “웹 서버에 대한 DDoS 공격의 네트워크 트래픽 분석”, 정보처리학회논문지 제10-C권,제3호, 2003. 6

〔8〕 전용희, 장종수, “비정상 트래픽 공격 유형 분석”, 한국정보보호학회논문지 Vol.17, No.2, pp80-89, 2007

〔9〕 William W. S. Wei, “Time Series Analysis”, Addison-Wesley, 1994

〔10〕 조강홍, 안성진, 정진욱, “ARIMA 모델을 이용한 선로 이용률의 임계값 위반 예측 기법”, 한국통신학회논문지 제25권, 제8호, 2000.8

〔11〕 http://www.unitel.co.kr/unitel/product/threatx/2006_threatex.htm

〔12〕 http://www.unitel.co.kr/unitel/product/smb/smb-index.htm

〔13〕 C.Zou, W. Gong, D. Towsley, and L.Gao, “The Monitoring and Early Detection of Internet Worms”, in Proc. 10th ACM conference on Computer and communication security, pp.190-199, 2003

〔14〕 정상준, 김동주, 권영헌, 김종근, “네트워크 트래픽 예측을 위한 시계열 모형의 적합성 검증”, 한국통신학회논문지 04-2 Vol.29 No.2B, pp.217-226, 2004



**조 강 홍** (Kang Hong Cho) 정회원

1997년 2월 성균관대학교 정보공학과 학사
1999년 2월 성균관대학교 전기전자 및 컴퓨터공학부 석사
2003년 2월 성균관대학교 전기전자 및 컴퓨터공학부 박사
2003년 3월~현재 동양공업전문대학 조교수
<관심분야> 트래픽 분석, 보안, QoS 라우팅

**이 도 훈** (Do Hun Lee) 정회원

1989년 2월 한양대학교 전산학과 학사
1991년 2월 한양대학교 전산학과 석사
1991년 2월~2000년 1월 국방과학연구소 선임연구원
2000년 3월~현재 국가보안기술연구소 팀장
<관심분야> 컴퓨터 통신, 네트워크 보안