Fisher 선형 분류법을 이용한 비정상 트래픽 탐지

Traffic Anomaly Detection for Campus Networks using Fisher Linear Discriminant

박 현 희*, 김 미 정**, 강 철 희*★
Hyunhee Park*, Meejoung Kim**, Chul-Hee Kang*★

Abstract

Traffic anomaly detection is one of important technology that should be considered in network security and administration. In this paper, we propose an abnormal traffic detection mechanism that includes traffic monitoring and traffic analysis. We develop analytical passive monitoring system called WISE-Mon which can inspect traffic behavior. We establish a criterion by analyzing the characteristics of a traffic training set. To detect abnormal traffic, we derive a hyperplane by using Fisher linear discriminant and chi-square distribution as well as the analyzed characteristics of traffic. Our mechanism can support reliable results for traffic anomaly detection and is compatible to real-time detection. In addition, since the trend of traffic can be changed as time passes, the hyperplane has to be updated periodically to reflect the changes. Accordingly, we consider the self-learning algorithm which reflects the trend of the traffic and so enables to increase the pliability of detection probability. Numerical results are presented to validate the accuracy of proposed mechanism. It shows that the proposed mechanism is reliable and relevant for traffic anomaly detection.

요 약

최근 인터넷을 통한 각종 침해사고 및 트래픽 폭주와 같은 현상이 급격하게 증가함에 따라 네트워크의 비정상적 상황을 조기에 탐지하기 위한 보다 능동적이고 진보적인 기술이 요구되고 있다. 본 논문에서는 캠퍼스 네트워크와 같이 트래픽이 주기적인 특성을 띠는 환경에서 Fisher 선형 분류법(FLD)을 사용하여 트래픽을 두 개의 그룹으로 분류하고, 네트워크에 유입되는 트래픽이 어떤 그룹에 속하는지를 판별하는 기법을 제안한다. 이를 위해 WISE-Mon이라 불리는 트래픽 분석 시스템을 개발하여 캠퍼스 네트워크의 트래픽을 수집하고 이를 모니터링해서 분석을 수행한다. 생성된 트래픽의 training set을 이용하여 비정상 트래픽의 범위를 판단하기 위한 chi-square distribution을 유도하고, FLD를 적용하여 유입되는 트래픽을 두 그룹으로 분리하기 위한 초평면 (hyperplane)을 만든다. 또한 네트워크 내의 트래픽 패턴이 시간이 지남에 따라 계속적으로 변하는 상황을 반영하기 위하여 self-learning 알고리즘을 적용한다. 캠퍼스 네트워크의 트래픽을 적용한 수학적 결과를 통하여 제안하는 기법의 정확성과 신뢰도를 보여준다.

Key words : Anomaly detection, traffic analysis, traffic measurement, Fisher linear discriminant

* 高麗大學校 電子컴퓨터工學部
(Department of Electronics and Computer Engineering, Korea University)
★ Corresponding author
** 고려대학교 정보통신기술연구소
※ 본 연구는 지식경제부 및 정보통신연구진흥원의 IT 핵심개발사업의 일환으로 수행하였음. [2008-F-006-01, 테라헤르츠 대역 근거리 무선 통신시스템 연구]
接受日:2009年 5月 4日, 修正完了日: 2009年 6月 20日

Ⅰ. 서론

오늘날의 통신 네트워크는 전통적인 인터넷 응용 프로그램뿐만 아니라 멀티미디어 스트리밍, P2P, 실시간 음성 및 화상 통신, 네트워크 게임 등 인터넷 기반 응용 프로그램들이 증가하면서 네트워크의 트래픽들이 복잡화되고 다양화되어 이에 대한 트래픽 모니

터링과 분석의 중요성이 대두되고 있다. 이렇게 복잡화되고 다양화된 네트워크를 통하여 비정상 트래픽의 발생과 각종 침해사고는 점점 증가하고 있으며 이로 인한 피해가 지속적으로 발생하고 있다. 비정상 트래픽은 네트워크 트래픽 폭주, DoS 공격, 웜과 같은 다양한 공격들의 원인이 되며 지능적이고 복합적인 형태로 발생되고 있기 때문에 이러한 이상 징후를 조기에 탐지할 수 있는 보다 진보된 기술이 요구되고 있다[1]-[2]. 따라서 기존의 많은 연구들이 비정상 트래픽을 탐지하기 위한 방법을 다루어 왔다.

대표적인 두 가지 방법으로는 rule 기반의 방식과 measurement 기반의 방식이 있다. 먼저 rule 기반의 방식은 비정상 트래픽의 패턴을 미리 파악해서 새롭게 발생하는 트래픽의 패턴은 미리 파악한 패턴을 비교해서 검출하는 방식이다[3]. 패턴 매칭과 같은 이러한 접근 방식은 알려진 공격에 대해서 높은 탐지율을 보인다. 그러나 알려지지 않은 새로운 공격에 대해서는 비교적 낮은 탐지율을 보이며, 패킷을 일일이 비교해야 하는 문제 때문에 백본과 같은 고속의 대용량 네트워크에서는 적합하지 않다는 단점이 있다. 이러한 단점을 극복하기 위하여 measurement 기반의 방식에서는 인터넷 백본 트래픽이 주기성을 띈다는 점을 전제로 하여, 네트워크 상에서 얻을 수 있는 간단한 트래픽 정보를 바탕으로 트래픽을 모델링함으로써 미래의 트래픽을 예측하는 방법과 많은 트래픽 정보 중 유용한 특정 정보들만을 샘플링하여 모델링하는 방법들이 제안되었다[4]-[7]. 그러나 모델링을 통해 탐지하는 방법은 정상의 여부만을 구분할 뿐 비정상의 종류를 알기 위해 여러 단계를 거쳐야 한다는 단점이 있다.

본 논문에서는 패턴 생성, 샘플링, 모델링 등 높은 오버헤드를 가지는 위의 접근 방식과는 달리 현재 추세를 직접적으로 반영하여 생성되는 기준면을 통해 비정상 트래픽을 분류하고 탐지하는 기법을 고려한다. 이 기법은 rule 기반의 패턴 매칭 기법[3] 보다 더 새로 발견된 이상적 현상을 정확히 탐지할 수 있고, measurement 기반의 시계열 분석의 모델링[4]과 같이 추이를 반영하기 위한 오버헤드와 비 실시간성을 효율적으로 극복할 수 있다.

이러한 비정상 트래픽의 탐지는 트래픽 모니터링이 중요한 부분을 차지하고 있기 때문에 트래픽의 특징을 잘 표현할 수 있는 파라미터들을 정의하고 트래픽 분석 시스템을 개발하는 것이 중요하다. 트래픽 모니터링 기술은 일반적으로 active 모니터링과 passive 모니터링으로 분류되는데 active 모니터링의 경우 delay, jitter, loss, bottleneck point, 사용가능한 bandwidth와 같이 네트워크 계층의 요소들을 위해 장비의 flow exporting 기능을 이용한 트래픽 정보 분석 방법이다. 반면에 passive 모니터링 기술은 네트워크에 지나다니는 모든 패킷을 관측하여 네트워크의 상태를 알아내는 기법이다. 이러한 모니터링 기술은 대용량의 트래픽을 취급하기 위한 문제와 다양하게 새로 생겨나는 응용 프로그램들을 다루기 위해 정확한 목적에 따라 계속적으로 발전해왔다[8].

캠퍼스 네트워크의 비정상 트래픽 탐지를 위해 우선적으로 WISE-Mon이라는 passive 트래픽 모니터링 및 분석 시스템을 개발했다. WISE-MON을 통해 수집된 트래픽의 집합은 training set으로 정의되며 이 집합과 Fisher 선형 분류법을 이용해 비정상 트래픽을 분리할 수 있는 기준면이 되는 hyperplane을 만들게 된다. 또한 변화하는 트래픽의 추세를 반영하여 새로운 hyperplane을 만들어내는 self-learning 알고리즘을 적용함으로써 비정상 트래픽 탐지의 정확도를 높였다.

본 논문의 구성은 다음과 같다. 2장에서는 Fisher 선형 분류법과 chi-square distribution에 관해 설명한다. 3장에서는 개발한 분석시스템에 대하여 언급하고 이를 이용한 트래픽 탐지기법을 제안한다. 4장에서는 실험 환경과 트래픽 분석 과정을 기술한다. 5장에서는 Fisher선형분류법을 이용해 만들어진 hyperplane을 통하여 비정상 트래픽을 탐지하고 제안한 탐지기법의 탐지율과 오탐율을 유도한다. 마지막으로 본 논문의 결론을 맺는다.

II. Preliminaries

이 장에서는 제안하는 기법의 기본이 되는 Fisher 선형 분류법과 chi-square distribution에 관하여 설명한다.

Fisher 선형분류법은 그룹 분류가 가능한 선형 함수로서 다차원 데이터를 hyperplane의 법선 벡터에 사영시켜 그룹을 분류하는 기법이다[9]-[10].

$X=\{\mathbb{X}_i=(x_{i1},\cdots,x_{in}):\mathbb{X}_i\in\mathbb{R}^n, i=1,\cdots,k\}$를 n개의 성분으로 이루어진 벡터로 구성된 데이터 집합이라 하자. 이 데이터 집합은 m 종류의 데이터로 그룹으로 분류된다고 가정하고, j그룹의 데이터 집합을 Y_j로 표기한다. 즉, $Y=\{Y_j\}_{j=1}^m$ 는 $\sum_{j=1}^{m}|Y_j|=k$를 만족하는 X의 disjoint subset이다. 여기서 $|A|$는 A집합의 원소의 개수를 나타낸다. $\boldsymbol{\mu}$와 $\boldsymbol{\mu}_j$는 각각 X와 Y_j의 평균이라 하자. 여기서 $\boldsymbol{\mu}=(\mu_1,\cdots,\mu_n)^t$와 $\boldsymbol{\mu}_j=(\mu_{j1},\cdots,\mu_{jn})^t$

의 성분은 각각 $\mu_l = \frac{1}{n}\sum_{i=1}^{n} x_{il}$와 $\mu_{jl} = \frac{1}{|Y_j|}\sum_{X_i \in Y_j} x_{il}$ 주어진다. 여기서 t는 행렬의 transpose를 나타낸 것이다.

이제 법선벡터(direction vector)를 소개하고 데이터 그룹 내의 산란행렬(scatter matrix)과 그룹 간의 산란행렬을 정의한다. 본 논문에서는 각 그룹의 평균 $\boldsymbol{\mu}_j$를 어떤 법선벡터 $\mathbf{w}$에 사영시켰을 때 각 그룹이 분리가 잘 될 수 있도록 최대의 분산을 갖게 하는 hyperplane $\mathbf{w}^t\mathbb{X}+d=0$ (여기서 $\mathbb{X}=(x_1,\cdots,x_n)$이고, d는 원점으로부터 hyperplane까지의 거리)과 수직인 법선 벡터 $\mathbf{w}$를 찾는 것이 목적이다. 그룹 내의 산란행렬과 그룹 간의 산란 행렬을 각각 $\mathbb{S}_{intra}$와 $\mathbb{S}_{inter}$로 나타낸다. 이 행렬들을 정의하기 위하여 $\mathbb{S}_j$를 집합 j의 산란행렬로 다음과 같이 정의한다.

$$\mathbb{S}_j = \sum_{\mathbb{X}_i \in Y_j} (\mathbb{X}_i - \boldsymbol{\mu}_j)(\mathbb{X}_i - \boldsymbol{\mu}_j)^t \quad (1)$$

이를 이용하여 $\mathbb{S}_{intra}$와 $\mathbb{S}_{inter}$는 다음과 같이 정의한다.

$$\mathbb{S}_{intra} = \sum_{j=1}^{m} \mathbb{S}_j,\ \mathbb{S}_{inter} = \sum_{j=1}^{m} (\boldsymbol{\mu}_j - \boldsymbol{\mu})(\boldsymbol{\mu}_j - \boldsymbol{\mu})^t$$

그러므로 각 그룹의 사영된 중심으로부터 그 그룹의 사영된 원소들 간의 정규화 된 분산의 합은 다음과 같이 나타난다.

$$\frac{1}{\|\mathbf{w}\|}\mathbf{w}^t\mathbb{S}_{intra}\mathbf{w},\ \frac{1}{\|\mathbf{w}\|}\mathbf{w}^t\mathbb{S}_{inter}\mathbf{w} \quad (2)$$

여기서 $\|\mathbf{w}\|$는 Euclidean norm을 나타내고, $\mathbf{w}^t\mathbb{S}_{inter}\mathbf{w}$은 계산하면 $\sum_{j=1}^{m}\left(\mathbf{w}^t(\boldsymbol{\mu}_j - \boldsymbol{\mu})\right)^2$이 된다.

그룹을 잘 분리하기 위하여 그룹 내의 데이터는 최대한 뭉쳐있어야 하고, 그룹간의 데이터는 최대한 멀리 떨어져 있어야 한다. 즉, 식 (2)의 값이 크다는 것은 그룹간의 구별이 명확하다는 것을 의미한다. 그러므로 식 (1)과 (2)를 이용하여 최적화 정식을 통한 classical Fisher criterion 함수를 다음과 같이 정의할 수 있다.

$$(\mathrm{OPT})\ \max_{\mathbf{w}\in D} OPT(\mathbf{w}) = \max_{\mathbf{w}\in D} \frac{\mathbf{w}^t\mathbb{S}_{\mathrm{inter}}\mathbf{w}}{\mathbf{w}^t\mathbb{S}_{\mathrm{intra}}\mathbf{w}}$$

여기서 $D=\{\mathbf{w}: \mathbf{w}^t\mathbb{X}+d=0, \mathbb{X}\in X\}$이다.

최적화 정식 (OPT)의 해는 분모를 최소화하고 분자를 최대화하여 얻을 수 있으므로, 각 그룹 내의 트래픽들은 동일한 특성들로 구성되어 있고 그룹간의 트래픽들은 서로 상이한 특성을 나타낼 수 있어야 한다. 최적화 정식은 다음과 같은 고유치 문제(eigenvalue problem)와 동치이다. (이 증명은 Appendix A에 나타나 있다.)

$$\mathbb{S}_{inter}\mathbf{w} = \lambda\mathbb{S}_{intra}\mathbf{w} \quad (3)$$

또한 식 (3)의 최대 고유값에 대응하는 고유벡터가 구하는 법선벡터 $\mathbf{w}$이다. ([9])

매일의 트래픽의 양은 크게 정규분포 (normal distribution)를 따름을 관찰할 수 있었으므로 이에 따라 30일 이상 수집한 데이터는 다음 정리에 의하여 카이스퀘어 분포 (chi-square distribution)을 따른다고 가정해도 크게 문제가 없을 것으로 보았다. 다음 정리는 표준정규분포 (standard normal distribution)와 카이스퀘어분포와의 관계를 나타내는데 이는 4절에서 사용될 것이다.

정리 1: 확률변수 $Z_1,\cdots,Z_k$가 각각 표준정규분포 $N(0,1)$을 따르고 서로 독립이면 $Z_1^2+Z_2^2+\cdots+Z_k^2$는 자유도 (degrees of freedom) k인 카이스퀘어 분포를 따른다. 이것은 $Z_1^2+Z_2^2+\cdots+Z_k^2 \sim \chi^2(k)$로 나타낸다 [7]-[8].

III. 제안하는 탐지 기법

네트워크 관리자의 입장에서 사용자에게 효율적이고 정상적인 서비스를 제공하기 위해서는 유해 트래픽 뿐 아니라 악의성은 없지만 네트워크 사용자가 정상적인 서비스를 제공받는데 문제가 되는 비정상 트래픽들에 대한 탐지가 이루어져야 한다. 또한 각각의 비정상 트래픽들은 네트워크의 특성에 따라서 정상 트래픽으로 분류되는 경우도 있을 수 있다. 예를 들면, 어떤 네트워크 안에서는 ftp 트래픽으로 인해 다른 정보 전송에 문제를 야기한다면 해당하는 ftp 트래픽은 비정상 트래픽으로 분류되어야 하고, 네트워크의 효율 측면에서 일정 수준의 ftp 트래픽만을 허용할 수 있다면 그보다 더 많은 양의 ftp 트래픽에 대해서는 비정상 트래픽으로 탐지를 해야만 제어할 수 있을 것이다. 이러한 관점에서 네트워크 트래픽들이 가진 특성에 따라 분류하고 유입되는 트래픽이 어떠한 트래픽의 그룹에 속하는지 분류을 하는 작업이 필요하다.

본 논문에서 제안하는 방법은 네트워크 상에서 관측되는 트래픽들이 지니고 있는 특성들을 성분으로

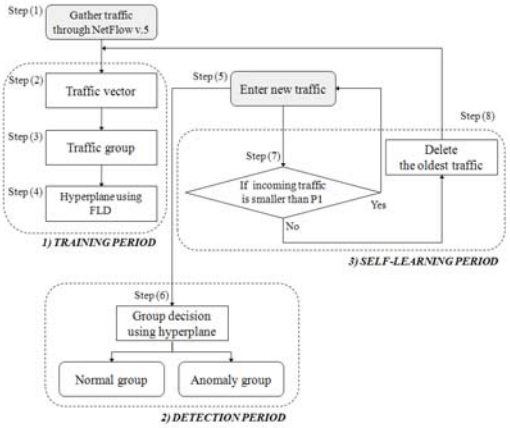

Fig. 1. The proposed detection mechanism
그림 1. 제안하는 탐지 기법

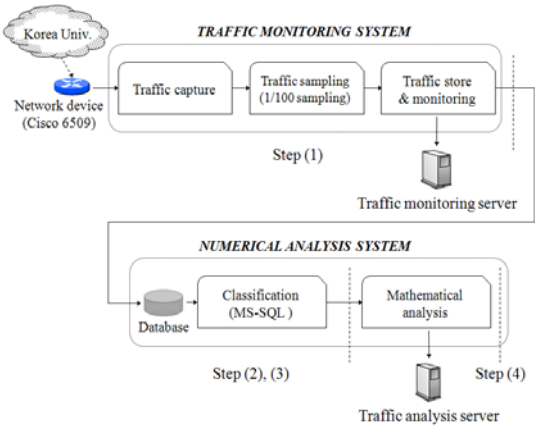

Fig. 2. Structure of the WISE-Mon
그림 2. WISE-Mon의 구성도

하는 데이터의 집합인 트래픽 벡터를 정의한 후 트래픽 벡터를 사용하여 위에서 언급한 바와 같이 트래픽을 그 특성에 따라 그룹을 짓고 그 그룹이 잘 구분이 되는지 판별한 후에 유입되는 트래픽이 어떠한 그룹에 속하게 되는지 탐지하는 방안을 제안하고 있다.

이 장에서 우리는 캠퍼스 네트워크 상의 비정상 트래픽을 탐지하기 위한 기법을 제안한다. 이 탐지 기법은 학습기간 (training period), 탐지기간 (detection period), 자기학습기간 (self-learning period)으로 구성된다. 이 기법을 구체적으로 설명하기에 앞서 몇 가지 용어를 정의한다.

정의 1: $\mathbb{X}=(x_1,\cdots,x_n)$는 트래픽의 정보를 성분으로 갖는 벡터이다. 이 $\mathbb{X}$를 트래픽 벡터 (traffic vector)라 부른다.

정의 2: $X=\{\mathbb{X}_i\}_{i=1}^{k}$중에서 동일한 특성을 갖는 트래픽 벡터들의 집합을 트래픽 그룹이라 한다. 앞에서 정의한 Y_j는 트래픽 그룹이다.

트래픽 벡터는 각 트래픽 그룹의 특성을 나타낼 수 있는 측정 가능한 항목들을 그 성분으로 가지며 그 성분은 router로부터 관찰되는 정보인 source(src) IP, destination(dst) IP, src port, dst port, protocol, flow 등이 될 수 있다. 또한 트래픽 그룹은 이러한 동일한 특성을 갖는 트래픽 벡터들의 모음이라 할 수 있다. 트래픽 그룹은 정상 (nornal) 그룹, 비정상 (abnormal) 그룹, 웜 (worm) 그룹, traffic congestion 그룹 등 여러 그룹으로 분류할 수 있고, 특히 비정상 그룹의 경우 네트워크오작동(network operation anomaly) 그룹, flash crowd anomaly group, 네트워크남용(network abuse anomaly) 그룹 등 구체적으로 세분화할 수 있다[12].

그림 1은 제한하는 탐지기법의 전체적인 동작을 보여준다. step (1)에서 step (4)는 트래픽을 모으고 분석하는 학습기간이다. 이 과정을 위해 우리는 WISE-Mon (Wide backbone network traffic Identification and Statistical Estimation Monitoring)이라 불리는 트래픽 모니터링 및 분석시스템을 개발하였다. 그림 2는 WISE-Mon의 전체적인 구성도를 나타낸다.

WISE-Mon은 크게 traffic monitoring system과 numerical analysis system의 구성된다. Traffic monitoring system은 traffic capture, traffic sampling, traffic store와 monitoring의 3가지로 구성되는 반면, numerical analysis system은 traffic classification과 mathematical analysis의 2가지로 구성된다. raw 데이터는 고려대학교 자연계 캠퍼스의 backbone 라우터(cisco 6509)로부터 수집한다. 이 raw 데이터는 Netflow v5의 형식으로 구성한다. Netflow는 기본적으로 단일방향의 특성을 가지며 출발지 및 도착지 주소와 포트번호, 프로토콜 등 5개의 튜플(tuple)로 구성된다. 그 외에도 TOS 및 인터페이스 정보, AS 정보를 포함한다. Netflow는 이러한 정보를 규칙으로 적용하여 다양한 프로토콜 플로우를 생성하고 구분할 수 있다. 이는 처리 속도가 빠르고 트래픽의 흐름과 동시에 라우터에서 생성되어 네트워크 관리자가 그 정보를 즉시 받아 볼 수 있다는 장점이 있다. raw 데이터는 1/100의 샘플링 과정을 거쳐 traffic monitoring server에 저장된다. 그림 1에서

step (2)와 (3)은 그림 2의 numerical analysis system에 의해 수행되는데, 데이터베이스 시스템은 트래픽을 매일 5분 단위로 생성하여 엑셀 파일 형식으로 저장하게 된다. 수집된 트래픽의 특성에 따라 트래픽 벡터의 성분을 결정하고 각 트래픽 벡터의 공통된 특성에 따라 트래픽 그룹을 결정하게 된다. 본 논문에서는 트래픽 그룹의 기준을 결정하기 위해 MS-SQL query를 이용하여 2개의 트래픽 그룹을 만든다. 그림 2의 mathematical analysis에서는 그 그룹의 정확한 기준을 만들기 위하여 카이스퀘어 분포을 적용하고, Fisher 선형 분류법을 통해 만든 hyperplane을 통해 트래픽을 탐지한다. 다음 단계는 탐지 과정이다. 그림 1의 step (5)에서 새로운 트래픽이 발생되었을 때, step (6)에서는 유도된 hyperplane에 의해 그 트래픽이 어떤 그룹에 속할지 판단할 수 있다. 그리고 step (7)에서 새롭게 발생하는 트래픽의 추이를 반영하기 위해서 자기학습 알고리즘을 적용한다. 업데이트 주기를 P1이라 했을 때, 가장 오래된 P1기간의 트래픽은 P1 기간 동안 새롭게 들어온 트래픽으로 교체된다.

Ⅳ. 트래픽 분석

이 장에서는 고려대학교의 백본 라우터를 통해 수집된 트래픽을 분석한다. 트래픽은 2008년 5월 14일 자정을 시작으로 매 5분 단위로 2008년 6월 12일 23:55분까지 30일 동안 수집하였다. 하루 288개의 관찰 시점으로 얻은 학습집합 (training set)은 총 8640개로 구성된다. 트래픽 벡터는 세 개의 성분을 가지며 그 성분은 bandwidth의 용량 (b), flow의 용량 (f), packet의 용량 (p)으로 정의하였다. 또한 그룹을 분리하기 위하여 정상그룹 (normal group)과 비정상그룹 (abnormal group)을 고려한다. 그림 3은 앞서 설명한 30일 동안 수집한 트래픽과 그의 일부인 하루 트래픽의 bandwidth의 양에 대한 경향을 보여준다. 이 그림을 통하여 우리가 주목해야할 점은 밤 11시부터 오전 6시까지는 매우 적은 량의 트래픽이 발생한다는 것인데, 이는 이 시간 자연계 캠퍼스의 모든 열람실이 닫기 때문에 나타나는 현상이라 볼 수 있다. 지면 관계상 flow와 packet의 그림은 생략하였으나 bandwidth와 거의 유사한 모습을 보였다.

학습 집합으로부터 두 개의 그룹을 분리하기 위한 기준을 만들기 위하여 수집한 트래픽의 분포를 관찰한다. 그림 4는 일일 데이터의 bandwidth 양의 분포이고, 그림 5는 30일간 수집한 데이터의 bandwidth 양의 분포를 나타내고 있다. 그림 4를 통하여 비록

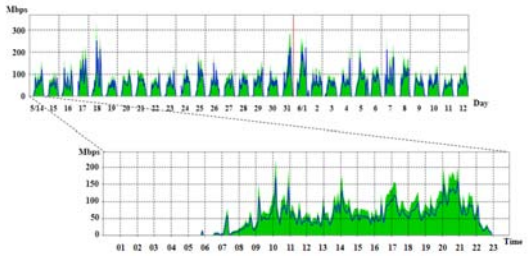

Fig. 3. 24-hour seasonal phenomenon of bandwidth
그림 3. Bandwidth 량의 24시간 현상

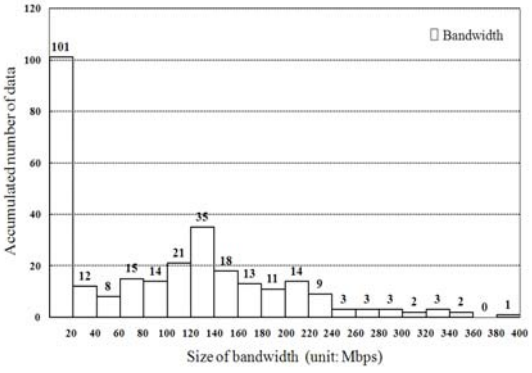

Fig. 4. Distribution of the size of bandwidth for one day traffic
그림 4. 일일 데이터의 bandwidth의 분포

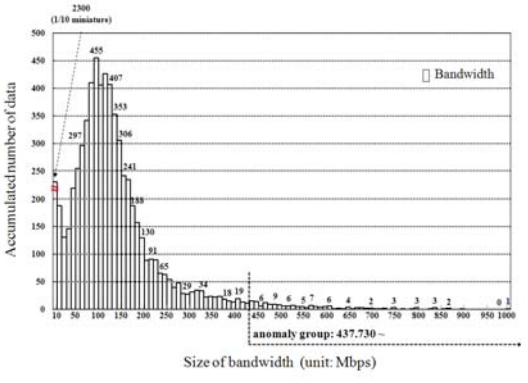

Fig. 5. Distribution of the size of bandwidth for 30 days aggregated traffic
그림 5. 30일 수집한 데이터의 bandwidth 양의 분포

연속적이지는 않지만 0~20Mbps를 제외한 일일 트래픽의 분포가 표준정규분포를 따름을 알 수 있다. 0~20Mbps를 제외한 이유는 밤 11시부터 오전 6시까지의 매우 적은 량의 데이터가 포함되어 있는데 이는

비정상 기준에 포함되지 않기 때문이다. 그림 5에 나타난 바와 같이 30일 동안 수집된 트래픽은 왼쪽으로 치우쳐 있고 오른쪽으로 긴 꼬리 모양을 갖는 카이스퀘어 분포를 따르고 있음을 알 수 있다. 일일 데이터가 표준정규분포를 따르고 이를 각각 제곱하여 더한 그래프가 카이스퀘어 분포를 따르고 있으므로 앞에서 이미 언급한 바와 같이 30일 동안의 데이터는 자유도가 30인 카이스퀘어 분포를 따른다고 가정해도 무방함을 알 수 있다. 이제 약 5%의 데이터가 전체 트래픽의 비정상 범위에 속한다고 가정하고 그룹을 나누기 위한 기준을 만들었다. 카이스퀘어 분포의 표(Table C.5, [11])를 참고하여 $\chi^2_{30;0.05,b}=43.7730$의 결과를 얻었다. 이는 437.730 Mbps 이상의 bandwidth 양을 가지는 트래픽은 비정상 범위에 속한다는 것을 의미한다. 이 기준에 의하면, 8640의 트래픽 중 8468개의 트래픽이 정상에 속하고, 남은 172개의 트래픽이 비정상 그룹에 속함을 알 수 있다. 나머지 flow와 packet도 각각 8617개와 8263개가 정상 그룹에 속함을 알 수 있었다. 또한 MS-SQL의 query에 OR조건을 적용하여 3개의 트래픽 벡터의 성분중 하나라도 비정상이라면 비정상 그룹에 속한다는 기준을 정하였다. 이 기준에 따라 정상그룹과 비정상 그룹이 각각 $|Y_n|=8241$와 $|Y_{an}|=399$으로 나타났다.

Ⅴ. 수학적 결과

이 장에서는 Fisher 선형분류법을 이용하여 hyperplane을 얻는 과정을 설명한다. 먼저 법선 벡터 **w**를 구하기 위해 각 그룹의 평균과 전체 평균을 모두 구하고, $\mathbb{S}_{intra}$와 $\mathbb{S}_{inter}$의 값을 각각 계산한다. 트래픽에 관한 각각의 평균은 표 1에 나타나 있다.
w를 찾기 위해 식 (1)에 주어진 고유값 문제의 특성방정식 $|\mathbb{S}_{intra}^{-1}\mathbb{S}_{inter}-\lambda\mathbb{I}|=0$을 이용한다.
방정식으로부터 3개의 다른 고유값과 그에 대응하는 고유벡터를 구한다.
이렇게 구한 고유값들 중 가장 큰 값에 대응하는 고유벡터가 법선벡터 **w**가 된다.

이제 이렇게 구한 법선벡터와 수직이고 평균점을

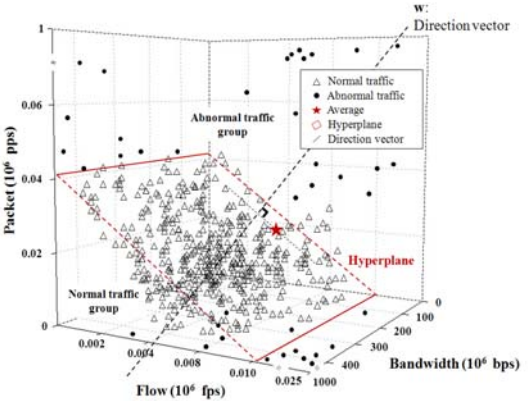

그림 6. 법선벡터 **w**, hyperplane, 두 개의 그룹, 평균점

$$\lambda_1=0.1882e^{002},\ \lambda_2=-0.1083e^{-14},\ \lambda_3=0.7932e^{-008}$$
$$\mathbf{w_1}=(-28.6341,-0.9995e^{-002},-0.4927)^t$$
$$\mathbf{w_2}=(0.2597e^{-003},-0.3358e^{-002},9.8352)^t$$
$$\mathbf{w_3}=(9995.6493,-0.1654e^{-002},-0.1577e^{-001})^t \quad (4)$$

지나는 평면을 구함으로써 찾고자 하는 hyperplane을 정의할 수 있다. 이에 따라 구한 hyperplane의 방정식은 다음과 같다.

$$-28.6341(x-103,709,872.7)-0.9995e^{-002}(y-5,247.040)$$
$$-0.4927(z-18,336.008)=0 \quad (5)$$

그림 6은 각각의 트래픽과 **w**, hyperplane, 분리된 두 개의 그룹을 보여준다. 앞에서 구한 법선벡터와 hyperplane, 그리고 그림을 단순화하기위해 정상 트래픽과 비정상 트래픽의 1/10만을 표현하였다. 이 hyperplane을 새로 유입되는 트래픽에 적용함으로써 그 트래픽이 아래 영역인 정상 그룹에 속하는지 위 영역인 비정상 그룹에 속하는지 판단할 수 있다.
이 hyperplane은 탐지하고자 하는 트래픽의 추세를 반영할 수 있도록 계속적으로 변하는 평균값과 hyperplane을 통해 실시간 탐지가 가능하다.

Table 1. Average of each group and total traffic.
표 1. 각 그룹과 전체 트래픽의 평균 값

average	bandwidth(bps)	flow(fps)	packet(pps)
average for normal traffic μ_n	μ_{nb}=87,945,088.43	μ_{nf}=5,220.758403	μ_{np}=12,951.99879
average for abnormal traffic μ_{an}	μ_{anb}=429,317,861.4	μ_{anf}=5,789.884712	μ_{anp}=129,538.0727
average for total traffic μ_{total}	$\mu_{total,b}$=103,709,872.7	$\mu_{total,f}$=5,247.040972	$\mu_{total,p}$=18,336.00845

abnormal traffic pattern	abnormal traffic type	dangerous level	amount of traffic	duration	interface of backbone router in Korea univ. network
	Jump (TrafficPps)	Critical	403.958	2008-07-02 21:37:00~ 2008-07-02 21:37:00	163.152.16.17 - HanaPark_16.17 (HanaPark_16.17) 163.152.16.47 - Vl217
	Jump (TrafficPps)	Critical	1160.620	2008-07-02 21:14:00~ 2008-07-02 21:35:00	163.152.16.17 - HanaPark_16.17 (HanaPark_16.17) 163.152.16.47 - Vl217
	Jump (TrafficPps)	Critical	901.967	2008-07-02 21:14:00~ 2008-07-02 21:35:00	163.152.16.17 - HanaPark_16.17 (HanaPark_16.17) 163.152.16.17 - Vl216
	Jump (TrafficPps)	Critical	1402.500	2008-07-02 20:12:00~ 2008-07-02 21:11:00	163.152.16.17 - HanaPark_16.17 (HanaPark_16.17) 163.152.16.17 - Vl216
	Jump (TrafficPps)	Critical	1200.720	2008-07-02 20:12:00~ 2008-07-02 21:11:00	163.152.16.17 - HanaPark_16.17 (HanaPark_16.17) 163.152.16.47 - Vl217
	Profile (HighPps)	Critical	1.696	2008-07-02 21:10:00~ 2008-07-02 21:10:00	163.152.16.17 - HanaPark_16.17 (HanaPark_16.17) 163.152.16.47 - Vl217

Fig. 7. Anormality through monitoring server
그림 7. 모니터링 서버에 의해 관찰된 비정상 트래픽

한편, 이렇게 구한 hyperplane의 신뢰성을 입증하기 위하여 특정 하루의 데이터인 2008년 7월 2일의 데이터를 이 hyperplane에 적용하여 실험해 보았다. 이 날은 대학의 1학기 성적이 공시되어 학교 포털시스템의 트래픽이 매우 혼잡한 날이었고, 학교 전산처에서 관찰된 트래픽의 추이로 보아 비정상적으로 폭주한 트래픽이 많았던 날로 입증된다. 그림 7은 모니터링 서버로부터 수집한 비정상성을 보인 테이블의 일부를 나타낸 것이다. 이 그림을 통하여 우리는 비정상적인 트래픽의 종류와 발생 시점, 그리고 그 패턴 등을 알 수 있다. 선택된 이 특정 하루에는 비정상적으로 보이는 jump 트래픽과 급격히 폭주하는 모습의 profile 트래픽이 많이 관찰되었고 이러한 비정상적 트래픽이 관찰되는 주기도 길고 빈번히 나타남을 알 수 있었다.

또한 새로 들어오는 트래픽을 5분 단위로 업데이트하여 기존의 가장 오래된 5분의 트래픽을 삭제하고 새로운 5분의 트래픽을 삽입하여 업데이트된 hyperplane을 만드는 자기학습 알고리즘을 제안하였다. 5분 단위로 계속해서 hyperplane을 업데이트하는 이유는 기존 바이러스나 공격과 달리 매우 빠른 속도로 침해사고를 일으키는 slammer worm과 같은 영향력 있는 공격을 차단하기 위해서이다[13]. Slammer worm은 출몰과 동시에 마이크로소프트(MS) SQL 데이터베이스 소프트웨어의 약점을 이용해 급속히 확산되었다. 이는 네트워크를 통해 자기 복제를 하며 이동하여 매 8.5초마다 두 배로 확산, 불과 10분만에 취약한 호스트의 90%를 감염시켰다. 전파 속도가 최고조에 달한 출현 후 3분 정도 되는 시점에선 인터넷 네트워크를 통해 초당 5천500만회의 위치 검색 요청 신호를 보낸 것으로 나타났다. 그림 8은 기존 2008년

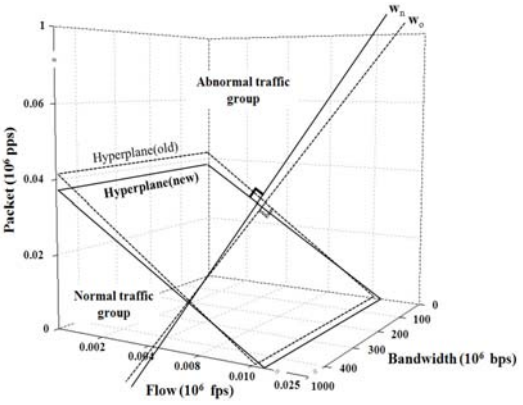

Fig. 8. The comparison of the original hyperplane and the updated hyperplane
그림 8. 기존 hyperplane과 update된 hyperplane과의 비교

5월 14일부터 5월 20일까지의 학습집합을 삭제하고 새로운 2008년 6월 13일부터 6월 19일까지의 일주일의 학습집합으로 교체해서 구한 hyperplane의 모습을 보여준다. 새로 형성된 hyperplane의 경향도 약간의 기울기만 변했을 뿐 거의 유사한 모습을 보임을 알 수 있다. 5분 단위의 hyperplane의 변화를 살펴보았을 때, 거의 유사한 모습을 보이므로 육안으로는 변화의 모습을 보일 수가 없어서 편의상 일주일 단위의 hyperplane 변화를 보였다. 이 그림을 통하여 새로 형성된 hyperplane의 경향도 약간의 기울기만 변했을 뿐 거의 유사한 모습을 보임을 알 수 있다.

이제 제안하는 기법의 성능을 평가하기 위해 다음과 같은 용어를 정의한다.

정의 3: 실제로 정상그룹에 속하면서 정상그룹으로 옳게 판단된 경우를 true positive라 한다. 실제로 비정상그룹에 속하면서 비정상그룹으로 옳게 판단된 경우를 true negative라 한다. 또한 실제로는 정상그룹에 속하나 비정상그룹에 속하는 것으로 잘못 판단된 경우를 false positive라 한다. 반면 실제로는 비정상그룹에 속하나 정상그룹에 속하는 것으로 잘못 판단된 경우를 false negative라 한다.

이제 얻어진 결과에 따라 탐지가 얼마만큼 정확한지를 알아보기 위해 다음과 같이 correct detection probability와 miss detection probability를 정의한다.

$$P_{cor} = \frac{|TP|+|TN|}{|\text{Total traffic}|},\ P_{mis} = \frac{|FP|+|FN|}{|\text{Total traffic}|} \qquad (7)$$

여기서 |FP|, |FN|, |TP|, |TN|는 각각 false positive, false negative, true positive, true negative를 나타낸다. 특정한 날을 기준으로 288개의 트래픽에 탐지과정을 적용하여 표 2와 같은 결과를 얻었다.

비정상 트래픽의 정보를 제공하는 학교 전산처 서버를 통해 보았을 때, 이 논문에서 고려한 특정한 날인 7월 2일에는 108개의 정상 트래픽과 180개의 비정상 트래픽이 있었음을 알 수 있었다. 한편, 이 논문에서 구한 hyperplane에 이 트래픽을 적용해 보았을 때 103개의 정상 트래픽과 185개의 비정상 트래픽을 탐지해 냈다. 표 2는 탐지율과 오탐율의 결과를 보여주고 있다. 표에서 보는 바와 같이 3%의 오탐률이 발생하였으며 이 오탐률은 flow량의 차이가 매우 적어 트래픽 그룹을 나눔에 있어 생긴 오차로 보인다.

본 논문에서 제안한 탐지기법의 성능을 알아보기 위하여 유사한 환경에서 비정상 트래픽 탐지를 다룬 [14]의 결과와 비교해 본다. 실험 데이터가 완전히 일치하지는 않으나 [14]에서는 Tunisian National University Network (TNUN)을 이용하여 비정상 트래픽을 탐지하였다. 이를 위하여 [14]에서는 45일간 주기적으로 캠퍼스 네트워크의 데이터를 수집하고 Anomaly Detection System (ADS)을 개발하였다. TNUN 중앙의 방화벽으로부터 MIB (Management Information Base)를 통해 네트워크 트래픽 trace들을 수집한다. 수집한 결과를 통하여 inter-anomaly 시간 분포와 anomaly duration 분포를 계산하여 5분 이내에 비정상 트래픽을 탐지하게 된다. 비록 같은 실험 데이터는 아닐지라도 TNUN의 트래픽도 본 논문에서 사용한 실험 데이터와 거의 유사한 실험 데이터를 사용하였다. 그 실험 결과, 본 논문에서 고려한 것과 동일한 탐지상황 하에서 약 90%의 탐지율을 보임을 알 수 있다. 즉, 이 결과와 비교했을 때 본 논문에서의 기법이 약 7% 우수함을 알 수 있다. 차후, 본 기법은 DARPA set과 같은 알려진 실험 데이터를 이용하여 기존의 여러 기법들과 비교할 것이다.

Table 2. Summary the detection information.
표 2. 탐지 결과에 대한 정리

Categories	normal group	abnormal group
using criterion for FLD	103	185
information from server	108	180
observed results	TP: 101, FN: 7, TN: 179, FP: 1	
probabilities	P_{cor}=0.97, P_{mis}=0.03	

Ⅵ. 결론

본 논문에서는 트래픽 벡터와 트래픽 그룹을 정의하고 Fisher 선형분류법에 의해 얻은 최적화된 hyperplane을 이용하여 새 트래픽 데이터가 생성되었을 때 그 데이터가 어떤 그룹에 속하는지를 결정하였다. 본 논문에서 제안한 방법은 기존의 방법에 비해 트래픽의 비정상 여부를 실시간으로 보다 간단하고 정확하게 탐지함을 알 수 있었다. 또한 트래픽 추이를 주기적으로 반영함으로서 새롭게 나타나는 이상적 현상을 탐지 할 수 있었다.

향후 본 연구는 트래픽 벡터에 새로운 성분을 추가하여 비정상 그룹을 좀 더 세밀한 비정상 그룹으로 분류하는 것으로 확장 것이다. 또한 실험 환경을 좀 더 큰 인터넷 백본 네트워크로 확장하여 제안하는 기법을 적용해 보아야 할 것이다.

Appendix A

최적화 정식(OPT)과 고유값 문제(eigenvalue problem)가 동치임을 증명한다.

증명: 다음과 같이 주어진 식 $OPT(\mathbf{w})$를 최대화하는 $\mathbf{w}$를 구하기 위하여

$$OPT(\mathbf{w}) = \frac{\mathbf{w}^t \mathbb{S}_{inter} \mathbf{w}}{\mathbf{w}^t \mathbb{S}_{intra} \mathbf{w}} \quad \text{(A1)}$$

식 (A1)의 양변을 $\mathbf{w}$에 대하여 편미분하면 다음과 같은 식을 얻는다.

$$\frac{\delta OPT(\mathbf{w})}{\delta \mathbf{w}} = \frac{(\mathbf{w}^t \mathbb{S}_{intra} \mathbf{w}) \mathbb{S}_{inter} \mathbf{w} - (\mathbf{w}^t \mathbb{S}_{inter} \mathbf{w}) \mathbb{S}_{intra} \mathbf{w}}{(\mathbf{w}^t \mathbb{S}_{intra} \mathbf{w})^2} \quad \text{(A2)}$$

식 (A2)가 0이 되는 $\mathbf{w}$는 다음과 같이 고유치 문제를 만족하는 고유 벡터가 된다.

$$\mathbb{S}_{inter} \mathbf{w} = OPT(\mathbf{w}) \mathbb{S}_{intra} \mathbf{w} \quad \text{(A3)}$$

참고문헌

[1] M. Thottan and C. Ji, "Anomaly Detection in IP Networks," IEEE Transaction on Signal Processing, vol. 52, no. 8, pp. 2191-2204, August 2003.

[2] S. S. Kim and A. L. N. Reddy, "Statistical Techniques for Detecting Traffic Anomalies Through Packet Header Data," IEEE/ACM

Transaction on Networking, vol. 16, no. 3, pp. 562-575, January 2008.
[3] R. Ahmed and R. Boutaba, "Distributed Pattern Matching: A Key to Flexible and Efficient P2P Search," IEEE Journal on Selected Areas in Communications, vol. 25, no. 1, pp. 73-83, January 2007.
[4] Y. W. Chen, "Traffic behavior analysis and modeling of sub-networks," International Journal of Network Management, vol. 12, pp. 323-330, September 2002.
[5] H. Hajji, "Statistical analysis of network traffic for adaptive faults detection," IEEE Transactions on Neural Networks, vol. 16, pp. 1053-1063, September 2005.
[6] G. Androulidakis and S. Papavassiliou, "Intelligent Flow-Based Sampling for Effective Network Anomaly Detection," in Proc. IEEE GLOBECOM 2007, pp. 1948-1953, November 2007.
[7] Z. Zhang and H. Shen "Online Training of SVMs for Real-time Intrusion Detection," in Proc. AINA 2004, pp. 568-573, March 2004.
[8] T. Hamada, K. Chujo, T. Chujo, and X. Yang, "Peer-to-peer traffic in metro networks: analysis, modeling, and policies," in Proc. IEEE/IETF NOMS 2004, pp. 425-438, April 2004.
[9] A. Shashua, "On the Relationship Between the Support Vector Machine for Classification and Sparsified Fisher's Linear Discriminant," Neural Processing Letters, vol. 9, pp. 129-139, April 1999.
[10] R. Johnson, and D.Wichern, Applied Multivariate Statistical Analysis, 6th ed., Prentice-Hall, 2007, pp. 576-593, 623-633.
[11] K. Trivedi, Probability and Statistics with Reliability, Queuing, and Computer Science Applications, 2nd ed., John Wiley and Sons, 2002, pp. 658-664.
[12] P. Barford and D. Plonka, "Characteristics of Network Traffic Flow Anomalies," in Proc. ACM SIGCOMM 2001, pp. 69-73, August 2001.
[13] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the Slammer worm," IEEE Security & Privacy Magazine 1(4), pp.33-39, July/Aug. 2003.
[14] K. H. Ramah, H. Ayari, and F. Kamoun, "Traffic Anomaly Detection and Characterization in the Tunisian National University Network," in Proc. NETWORKING 2006, LNCS 3976, pp.136-147, May 2006.

저 자 소 개

박 현 희 (학생회원)

2002년 : 한국항공대학교 통신정보공학과 졸업 (공학사)
2002년 9월~현재 : 고려대학교 대학원 전자·컴퓨터공학과 석·박사 통합과정
<주관심분야>
근거리 무선 통신, 무선 네트워크, 차세대 인터넷 기술, 네트워크 보안, 트래픽 모니터링 및 분석, 미래 인터넷
hyunhee@widecomm.korea.ac.kr
parkhyunhee@mail.com

김 미 정 (비회원)

1986년 : 고려대학교 수학과 졸업 (공학사)
1988년 : 고려대학교 대학원 수학과 (이학석사)
1993년 : University of Minnesota (이학박사수료)
1996년 : 고려대학교 대학원 수학과 (이학박사)
2000년~2004년 : BK21 정보기술사업단 연구교수
2004년 9월~현재 : 고려대학교 정보통신기술공동연구소
<주관심분야>
무선 멀티미디어 통신 시스템, 자원 관리, 매체 접근 제어, 무선 보안, 백색 잡음 분석

강 철 희 (비회원)

1975년 : 와세다대학교 전자통신 공학과 졸업 (공학사)
1977년 : 와세다대학교 대학원 전자통신공학과 (공학석사)
1980년 : 와세다대학교 대학원 전자통신공학과 (공학박사)
1980년~1994년 : 한국전자통신연구소
1980년~1983년 : 한국과학기술원(KAIST) 전기 및 전자과 / 기계공학과 대우교수
1991년~1994년 : 충남대학교 전자공학과 겸임교수
1994년~1995년 : Washington Univ. In.St. Louis 방문교수
1995년 3월~현재 : 고려대학교 전자공학과 정교수
<주관심분야>
차세대 인터넷 기술, 무선 네트워크, 유비쿼터스 컴퓨팅, 모바일 네트워크, 네트워크 보안