Journal of The Korea Society of Computer and Information
Vol. 17 No. 5 , May 2012

2012-17-5-2-1

선형패턴과 명암 특징을 이용한 네트워크 트래픽의 이상현상 감지

장석우*, 김계영**, 나현숙**

Detecting Abnormal Patterns of Network Traffic by Analyzing Linear Patterns and Intensity Features

Seok-Woo Jang*, Gye-Young Kim**, Hyeon-Suk Na**

요 약

최근 들어, 네트워크 트래픽 공격에 대한 탐지 기술의 필요성이 꾸준히 증가되고 있는 실정이다. 본 논문에서는 네트워크 트래픽 데이터의 헤더파일에서 송신자의 IP와 포트, 그리고 수신자의 IP와 포트 정보를 2차원의 영상으로 시각화하고 분석하여 이상패턴을 효과적으로 분석하는 새로운 방법을 제안한다. 제안된 방법에서는 먼저 송신자와 수신자의 IP 정보를 받아들여 4개의 2차원 영상을 생성하고, 포트 정보를 받아들여 1개의 2차원 영상을 생성한다. 그런 다음, 각 영상 내의 트래픽 데이터를 분석하여 패턴의 주요 특징을 추출하는데, 트래픽의 공격을 나타내는 선형 패턴과 높은 명암값을 가지는 패턴을 추출하여 트래픽의 유형이 정상 트래픽, DDoS, 그리고 DoS인지를 자동으로 검출한다. 성능을 비교 분석하기 위한 실험에서는 제안된 네트워크 트래픽의 이상현상 검출 방법이 기존의 방법에 비해서 보다 우수하다는 것을 보여준다.

▸ Keyword : 네트워크 트래픽, 이상 패턴, 시각화 기법, 명암 특징

Abstract

Recently, the necessity for good techniques of detecting network traffic attack has increased. In this paper, we suggest a new method of detecting abnormal patterns of network traffic data by visualizing their IP and port information into two dimensional images. The proposed approach first generates four 2D images from IP data of transmitters and receivers, and makes one 2D image from port data. Analyzing those images, it then extracts their major features such as linear patterns or high intensity values, and determines if traffic data contain DDoS or DoS Attacks. To comparatively evaluate the performance of the proposed algorithm, we show that our abnormal

• 제1저자 : 장석우 • 교신저자 : 나현숙
• 투고일 : 2012. 01. 17, 심사일 : 2012. 01. 24. 게재확정일 : 2012. 02, 10.
* 안양대학교 디지털미디어학과(Dept. of Digital Media, Anyang University)
** 숭실대학교 컴퓨터학부(School of Computing, Soongsil University)

pattern detection method outperforms the existing algorithm in terms of accuracy and speed.

▸ Keyword : Network Traffic, Abnormal Pattern, Visualization Technique, Intensity Feature

I. 서 론

네트워크 기술의 발전과 인프라의 급속한 확산으로 인해서 현대사회는 인터넷이 없는 세상을 상상할 수도 없게 되었다. 다시 말해, 경제, 사회, 문화, 그리고 교육 등에 관련된 수많은 서비스를 인터넷을 통해서 제공받을 수 있으며 인터넷을 이용한 다양한 활동들이 지속적으로 시도되고 있다. 그러나 인터넷의 이러한 많은 장점과 더불어 단점 또한 존재하는데 네트워크를 통한 공격(attack)이 그 중의 하나이다. 인터넷의 급속한 확산과 함께 네트워크의 공격은 나날이 증가하고 있으며, 공격의 성격도 단순하고 악의적인 목적에서 협박을 통한 금품갈취 등의 용도로 사용되는 등 여타 다른 범죄와 혼합되어 나타나는 양상을 보이고 있다.

이와 같이 사회 전 분야의 네트워크 의존화가 극대화에 다다른 오늘날 네트워크 트래픽 공격은 네트워크를 사용하는 모든 사업체에게 큰 위협이 되고 있으며, 최근에는 그 공격의 대상이 사업체에서 점점 국가 차원으로 확대되고 있으므로 각 국가에서도 무시할 수 없는 심각한 문제가 되었다. 따라서 네트워크 공격에 대한 방어 및 탐지 기술이 최근 들어 절실히 요구되고 있는 실정이다[1].

따라서 이러한 피해를 막기 위해 인터넷 상의 방대한 트래픽 데이터들을 효과적으로 분석하고 악성 공격 트래픽을 인지하여 대응하는 것이 매우 중요하다. 그러나 수많은 정보 중에서 자신이 원하는 정보만을 빠르게 분석하고 탐지하는 것은 그렇게 쉽지 않다. 최근에는 사이버 공격들의 형태가 점점 더 다양해지고, 공격의 전파 속도가 빨라짐에 따라 기존의 침입 탐지 기법으로는 이러한 공격을 신속하게 탐지하고 차단하기에는 한계가 있다. 이와 같은 문제점을 해결하기 위해서 최근에는 네트워크 보안 상황을 신속하게 분석하기 위한 방법에 관한 연구가 활발히 진행되고 있다.

보안 이벤트 시각화(visualization) 기술은 네트워크 상에서 발생되는 방대한 양의 이벤트를 실시간으로 시각화하는 기술로서 네트워크 관리자에게 보안과 관련된 많은 정보를 신속하고, 쉽고, 정확하게 전달할 수 있다는 장점이 있다. 네트워크 관리자는 보안 이벤트 시각화 기술을 사용하여 현재 네트워크에서 발생되는 트래픽(traffic)의 흐름 및 경보 메시지를 파악하고, 그 이상현상(anomaly)을 유발한 트래픽의 특성을 빠르게 분석하여 이 이상현상이 실제 네트워크 공격인지 아닌지를 신속하게 판단할 수 있다.

그리고 국내외적으로 다양한 보안 이벤트의 시각화를 통한 상황인지 기술이 보안 관리에 있어서 화두가 되고 있다. 상황인지 기술이란 각 객체의 진위를 판단하고 규명하기 보다는 그것들의 연관성과 전체적인 패턴 동향들을 통해 어떤 일이 발생하고 있고, 무엇을 해야 하는지를 알고자 함에서 출발한다[2]. 보안 이벤트 상황인지 기술을 사용하면 서비스 거부공격(DoS: Denial of Service), 분산 서비스 거부공격(DDoS: Distributed DoS), 인터넷 웜(Internet Worm), 포트 스캔(Port Scan) 등의 네트워크 공격에 대한 패턴을 잘 표현할 수 있기 때문에 네트워크 공격을 직관적으로 인지할 수 있다.

본 논문에서는 트래픽 데이터의 헤더 파일을 시각화 기법을 이용하여 2차원 영상으로 시각화하여 분석함으로써 이상현상을 자동으로 탐지하는 새로운 방법을 제안한다. 그림 1은 본 논문에서 제안하는 방법의 전체적인 개요도를 보여준다.

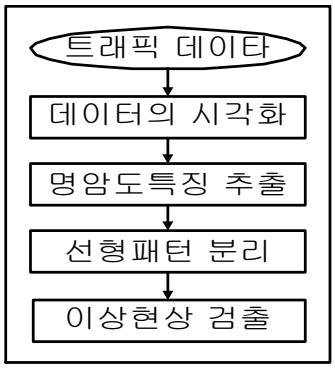


그림 1. 전체 개요도
Fig. 1. Overall Flow

1장에서는 본 연구를 수행하게 된 동기 및 배경, 그리고 전체적인 개요를 기술하였다. 2장에서는 네트워크 트래픽의 이상현상을 감지하는 관련연구에 대해서 기술한다. 3장에서는 트래픽의 시각화와 특징 분석에 대해서 기술한다. 4장에서는 패턴분석을 통해서 이상현상을 검출하는 방법 대해 기술한다. 그리고 5장에서는 본 논문에서 제안된 방법의 성능을 평가하기 위해서 수행한 실험결과를 보이며, 6장에서는 결론 및 향후 연구방향을 제시한다.

II. 관련연구

기존에 연구된 트래픽 폭주 공격 탐지에서의 패킷 수집 방법[3]은 공격에 대한 상세한 분석은 가능하지만 실시간으로 빠른 탐지가 어렵다는 문제점을 가지고 있다. 그리고 기존에 제안된 유해 트래픽 분석 방법[4]은 트래픽 발생시 SNMP(simple network management protocol)를 이용하여 트래픽을 수집하고, 수집된 트래픽에 대하여 프로토콜별 MIB(management information base) 객체 정보를 통하여 정상 트래픽과 공격 트래픽에 대해 분석한다. 따라서 최근 SNMP에서의 MIB 정보를 이용한 침입탐지 방법론이 주목을 받고 있다. 또한 이와 관련된 많은 연구들이 활발히 진행되고 있으며 계속해서 새로운 방법론이 제안되고 있다.

SNMP MIB 기반의 공격탐지 방법은 프로토콜별 추이분석, 일주 트래픽 추이분석, 그리고 MIB 에서의 특정 객체와 객체 정보 간의 상관관계를 이용하여 공격 트래픽을 탐지한다. 프로토콜별 추이분석은 시스템에서 발생하는 트래픽 정보를 수집하여 하루 동안 시간대별로 프로토콜의 분포를 예측하여 기준 값을 설정하고 현재 발생되는 트래픽의 프로토콜 분포와 비교하여 공격 트래픽을 탐지하는 방법이다. 그러나 이 방법은 신속하게 변화하는 네트워크 공격을 대응하기에는 한계가 있고 다양한 네트워크 트래픽에 대한 예측이 어렵다는 단점을 지니고 있다. 일주 트래픽 추이분석은 일분 또는 수십분 단위로 MIB 정보를 일정 기간 동안 수집한 후 모든 트래픽을 수용할 수 있는 기준 트래픽 추이 데이터를 설정하는 방법이다. 즉, 일정 시간 동안의 트래픽의 흐름을 예측하고 예측된 값과 현재 발생되는 트래픽을 비교하여 공격 트래픽과 정상 트래픽을 분류하는 방법이다. 이 방법은 임계값을 설정하는데 어려움이 많고 부동한 임계값을 사용함으로써 여러 가지 결과가 나타난다. MIB 객체 정보 간의 상관관계를 이용하여 공격 트래픽을 탐지하는 방법은 비교적 정확한 공격 트래픽 탐지에는 도움이 된다. 그러나 객체 정보 간의 상관관계를 정의해야 할 뿐만 아니라 별도로 연산하고 처리하기 위한 시간과 처리된 결과 값을 저장하고 관리하기 위한 추가적인 리소스를 요구하기 때문에 시스템의 안전성을 보장하기 위한 실시간 탐지가 어렵다는 단점을 가지고 있다[5]. 또한 기존의 MIB 기반의 공격탐지 시스템들은 대부분 기존의 기능과 특성에 의존적으로 개발된 시스템으로서 새로운 공격 유형이나 끊임없이 발전하는 공격 유형에 대처하기 어렵다[6]. 결과적으로 보면 실시간으로 새로운 유형의 공격을 탐지하는 방법과 탐지된 공격의 유형을 각각 분류할 수 있는 방법이 요구되며, 이런 모든 기능은 자동으로 진행이 가능한 기능이 보장되는 보다 안전하고 효율적인 방법이 요구되고 있다.

본 논문에서는 인터넷 트래픽 공격 중에서 가장 흔히 발생하는 DDoS와 DoS의 2가지 종류의 공격에 대해서 자동적으로 탐지를 수행하는 방법을 제안한다. 우선 각각의 공격 특징에 대해 설명하면 아래와 같다.

DDoS 공격[7]은 다수의 감염된 호스트가 피해 호스트에게 다량의 무의미한 패킷을 전송하여, 피해 호스트와 인터넷 사이의 자원 불균형을 초래한다. 여러 대의 공격자를 분산 배치하여 동시에 동작하게 함으로써 특정 사이트를 공격하는 방식이다. 분산 서비스 공격은 여러 개의 부동한 송신자 IP가 동시에 하나의 수신자 IP를 공격하기 때문에 송신자 IP와 수신자 IP의 관계는 N:1이다.

DoS 공격은 피해 호스트가 인터넷에서 정상적인 서비스를 제공하거나 서비스를 받는 것을 방해하는 공격이다[8]. 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격이다. 특정 서버에게 수많은 접속 시도를 만들어 다른 이용자가 정상적으로 서비스 이용을 하지 못하게 하거나, 서버의 TCP 연결을 바닥내는 등의 공격이 이 범위에 포함된다. DoS 공격은 한 대의 송신자 컴퓨터가 여러 포트를 이용하여 한 대의 수신자 컴퓨터에 접속한다는 것이다. 따라서 송신자와 수신자 IP의 관계는 1:1이고, 포트의 관계는 N:1 이다.

III. 트래픽의 시각화 및 특징분석

본 논문에서는 트래픽 데이터의 IP와 포트 정보의 특성을 이용하여 네트워크 트래픽을 2차원의 영상으로 시각화한다. 현재 사용하고 있는 대부분의 IP 주소는 0에서 255 사이의 범위를 가지는 4개의 숫자로 구성되어 있다. 그리고 포트 번호는 0에서 65,535 사이의 범위를 가지는 하나의 숫자로 구성된다.

먼저, IP 정보의 시각화를 생각해 보자. 만일, IP 주소가 A.B.C.D로 구성되었다고 가정한다면 본 논문에서는 그림 2와 같이 두 개의 2차원 영상으로 하나의 송신자 또는 수신자 IP 주소를 표현한다. 그림 2 (a)에서 a축은 IP 주소의 A 클래스, b축은 IP 주소의 B 클래스, 그리고 그림 2 (b)에서 c축은 IP 주소의 C 클래스, d축은 IP 주소의 D 클래스를 의미한다. 그림 2에서 표현한 것처럼 실제의 IP 주소 120.230.38.177을 시각화 할 때, a축과 b축을 나타내는 2차원 영상에서 해당 위치에 하나의 점으로 나타내고, c축과 d축을 나타내는 2차원 영상에서 해당 위치에 하나의 점으로 표현한다.

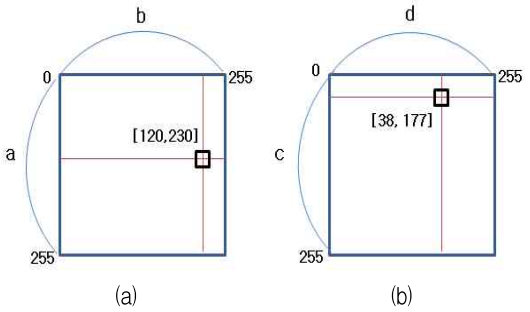


그림 2. IP 시각화
Fig. 2. IP Visualization

그리고 포트의 시각화는 그림 3 (a)와 같이 표현한다. 보통, 포트는 0에서 65,535 사이의 범위를 가지는 하나의 값을 가지기 때문에 65,536×65,536 크기의 영상을 만들기는 부담스럽다. 따라서 각 포트 번호를 0에서 255 사이의 숫자로 정규화한 다음 이를 영상으로 시각화한다.

그림 3 (b)는 송신자 포트와 수신자 포트를 이용한 실제 시각화의 예를 보여준다. 포트 시각화 방법을 이용하면 송신자와 수신자 사이의 포트 관계를 직관적으로 2차원 영상을 통해 알 수 있기 때문에 네트워크 트래픽 공격의 유무를 용이하게 판단할 수 있다. 그러나 포트 영상은 0에서 65,535 사이의 숫자를 0에서 255 사이의 값으로 정규화, 즉 65,536개의 데이터를 256개로 압축하는 과정을 거쳤기 때문에 정확도 측면에서 오차가 발생한다.

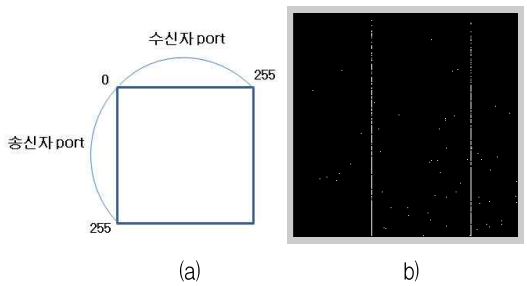


그림 3. 포트 시각화
Fig. 3. Port Visualization

IP에 대한 영상으로부터 임의의 송신자가 어떤 수신자들에게 접근하였는지, 그리고 얼마나 많이 접근하였는지를 패턴 형태와 명암도 분석을 통해서 알 수 있다. 본 논문에서는 IP 영상에서 검출할 수 있는 공격의 종류를 DDoS와 DoS의 2가지 종류로 구분하였으며, IP 영상에서 나타나는 각각의 공격 특징은 다음과 같이 기술할 수 있다.

그림 4의 DDoS 공격에 대한 트래픽 영상을 살펴보면 송신자 IP의 AB와 CD 영상에서 수많은 송신자들이 수신자 IP의 AB와 CD 영상의 한 수신자에게 집중되어 있는 모습을 볼 수 있다. 따라서 DDoS 공격이 수행되었는지의 여부는 송신자 IP의 영상에 선형의 패턴이 존재하는지, 또는 명암값이 높은 패턴이 존재하는지를 확인하여 공격의 유무를 판단하고 이에 대한 특징 값을 추출할 수 있다.

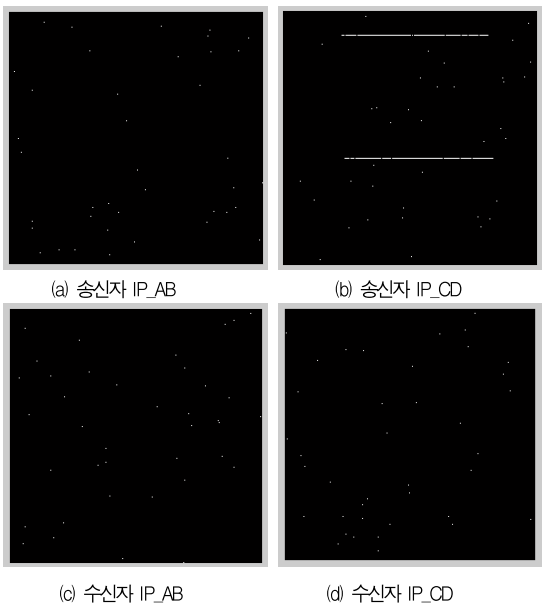
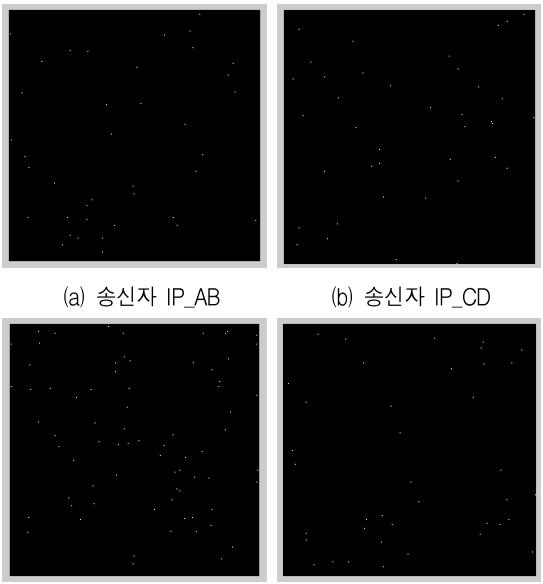


그림 4. DDoS의 IP 영상
Fig. 4. IP Image of DDoS

그림 5는 가상으로 수행한 DoS 공격 트래픽의 IP 영상이다. DoS 공격에 대한 트래픽 IP 영상을 보면 각 영상에서는 선형 패턴을 찾아볼 수 없다. 그러나 명암 값 측정을 통해 유난히 높은 명암 값을 갖는 IP를 탐지할 수 있을 것이다. 명암값이 높은 해당 IP가 바로 공격자와 희생자를 의미한다. 하나의 송신자가 일반적인 전송량을 벗어난 수많은 양의 데이터를 전송하여 하나의 수신자를 접속하기 때문에 매우 높은 명암값을 갖는 영역이 각 영상에서 모두 나타나게 된다. 이러한 특징을 통해 DoS 공격을 탐지할 수 있다.

포트 영상에서 나타나는 공격의 특징은 각각 아래의 그림 6과 같다. 보통, 포트 영상의 특징은 0에서 65,535 사이의 값을 가지는 하나의 숫자를 0에서 255 사이의 값으로 정규화하였다. 포트 영상은 y축은 송신자 포트, 그리고 x축은 수신자 포트로 구성된 하나의 2차원 영상으로 시각화된다. 이와

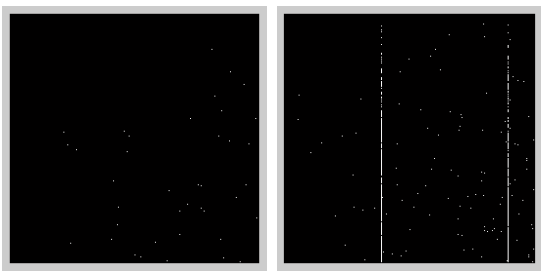


(a) 송신자 IP_AB (b) 송신자 IP_CD

(c) 수신자 IP_AB (d) 수신자 IP_CD

그림 5. DoS의 IP 영상
Fig. 5. IP Image of DoS

같이 생성된 2차원 포트 영상을 통해서 직관적으로 송신자 포트와 수신자 포트의 관계를 바로 알 수 있다. 만약, 여러 개의 송신자 포트가 하나의 수신자 포트에 접속하였을 경우 영상에서는 수직 방향의 선형패턴이 나타나게 된다. 이런 시각화 방법을 통해 송신자와 수신자 포트의 패턴 특징을 추출할 수 있다.



(a) DDoS (b) Dos

그림 6. 포트 영상
Fig. 6. Port Image

IV. 패턴분석에 의한 이상현상 검출

네트워크 트래픽 영상에서 나타나는 공격의 형태는 선형 패턴 또는 높은 명암 값을 갖는 패턴이다. 이 두 가지의 특징을 추출하여 공격을 판단하는데 선형 패턴의 가장 큰 특징은 선의 길이이다. 선형 패턴의 길이가 점과 유사할 정도로 짧다면 해당 선형 패턴은 공격 패턴보다는 일반적인 패턴일 가능성이 높으며, 반대로 선형 패턴의 길이가 길다면 해당 트래픽은 네트워크 공격일 가능성이 크다. 따라서 선형 패턴의 길이를 산출하면 공격의 발생 여부를 간단하게 추측할 수 있다. 그러나 시간의 흐름에 따라 네트워크 이벤트 영상이 갱신됨에 있어 선형 패턴이 일정하게 이어지지 않고 군데군데 끊어지는 현상이 발생할 수 있다. 이러한 경우에는 직선의 길이를 정확하게 판단할 수 없기 때문에 본 논문에서는 선형 패턴의 길이를 보다 정확하게 측정하기 위해서 허프 변환(Hough transform)을 사용하여 선형 패턴을 검출한다.

허프 변환은 영상에서 특징점들로 이루어진 직선, 원, 타원 등의 인자화된 곡선을 발견하기에 유용한 변환방법이다[9]. 허프 변환을 수행하는 가장 일반적인 방법은 각 특징점에서 각도 θ를 N개의 일정한 구간으로 나누어 샘플링한 각도 θ_i $(i=1,2,...,N)$을 가지는 직선들을 구하고, 각 직선에 해당하는 ρ를 직선의 방정식으로부터 구한 후, 이를 M개의 구간으로 양자화하여 해당하는 셀의 숫자를 증가시키는 방법이다. 이렇게 하여 구해진 허프 공간은 $M\times N$개의 셀들로 이루어지게 되고, 이 셀들 중 빈도가 일정한 임계값 이상이 되는 경우에 그 셀에 해당하는 직선이 존재한다고 판단한다.

본 논문에서는 IP와 포트 영상 각각에 대해서 선형 패턴을 탐지하고 그 길이를 측정하여 영상에서 가장 긴 선형 패턴과 선형 패턴의 길이를 산출한다. IP 영상에서 산출된 선형 패턴의 최대 길이는 256의 값을 가지므로, 식 (1)을 이용하여 최대 길이로 나누어 0과 1사이의 값으로 정규화한다. 포트 영상도 256×256의 크기로 정규화하였기 때문에 IP 영상과 같은 방법으로 식 (1)을 이용하여 가장 긴 선형 패턴을 최대 길이로 나누어 0과 1사이의 값으로 정규화한다.

식 (1)의 L은 선형 패턴의 최대길이를 의미하며, F_l은 선형 패턴에서 추출한 특징 값을 의미한다.

$$F_l = \frac{\max(L(i))}{256} \quad (1)$$

$$F_b = \frac{\max(p(x,y))}{N} \quad (2)$$

명암도가 높은 화소의 패턴 특징을 추출하기 위해서 본 논문에서는 트래픽 영상에 존재하는 화소의 명암 값 중에서 가장 큰 명암 값을 추출하여 특징으로 사용한다. IP와 포트 영상 각각에 대해 최대 명암 값을 추출한다. 그리고 추출된 명암 값은 식 (2)와 같이 패킷의 총 개수로 나누어 0과 1사이로

정규화한다. 식 (2)에서 N은 패킷의 총 개수를 의미하며, p는 해당 (x, y) 좌표의 화소의 명암값을 의미한다.

본 논문에서는 송신자와 수신자 IP, 포트 영상 각각에 대해 최대 명암값, 선형패턴의 최대길이, 선형패턴의 평균길이, 선형패턴의 개수를 추출하여 네트워크 트래픽의 이상현상 검출에 활용한다.

V. 실험결과

본 논문의 실험을 위해 사용한 컴퓨터는 인텔 Pentium-4 3.0Ghz의 CPU와 1GB의 메모리를 사용하였고, 운영체제는 마이크로소프트사의 윈도우 XP SP3를 사용하였다. 그리고 구현을 위해 사용한 언어는 마이크로소프트사의 Visual C++ 2008이다. 그리고 네트워크 트래픽의 이상현상을 검출하기 위한 실험 데이터로는 트래픽의 공격 특징별로 각각 100개의 데이터를 인위적으로 만들어 사용하였다.

표 5와 표 6은 정상 트래픽과 네트워크 트래픽 공격 패턴 특징값의 실제적인 예를 보여준다. 이는 여러 단계의 전처리 과정을 거쳐 최종적으로 추출한 특징 값이다. 이 값을 이용하여 네트워크 공격 발생 유무의 탐지를 수행한다.

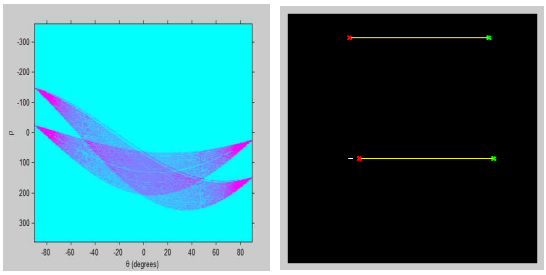
표 1. 정상 트래픽의 패턴특징
Table 1. Pattern of Normal Traffic

	최대명암값	선형패턴 최대길이	선형패턴 평균길이	선형패턴개수
송신자IP1	0.0250	0.0000	0.0000	0.0000
송신자IP2	0.0100	0.0000	0.0000	0.0000
수신자IP1	0.0390	0.0000	0.0000	0.0000
수신자IP2	0.0320	0.0000	0.0000	0.0000
포트 영상	0.0120	0.0000	0.0000	0.0000

표 2. DDoS 공격의 패턴특징
Table 2. Pattern of DDoS Attack

	최대명암값	선형패턴 최대길이	선형패턴 평균길이	선형패턴개수
송신자IP1	0.4850	0.0000	0.0000	0.0000
송신자IP2	0.0100	0.5390	0.3252	0.4000
수신자IP1	0.4390	0.0000	0.0000	0.0000
수신자IP2	0.4920	0.0000	0.0000	0.0000
포트 영상	0.0120	0.0000	0.0000	0.0000

그림 7은 허프 변환을 이용하여 시각화된 네트워크 트래픽 데이터로부터 선형 패턴을 탐지한 결과를 보여준다. 그림 7의 (a)는 입력된 시각화된 트래픽 영상에 대한 허프 공간을 보여주고, (b)는 입력된 영상으로부터 두 개의 선형 라인을 검출한 결과를 보여준다.



(a) (b)

그림 7. 선형 패턴 감지
Fig. 7. Detection of Linear Patters

기존의 MIB 트래픽 분석 방법[10]과 본 논문에서 제안한 방법을 이용한 공격탐지의 소요시간을 비교한 결과, 기존의 MIB 트래픽 분석 방법을 이용한 공격탐지는 공격과 정상 데이터의 두 가지 종류만을 분류할 수 있다. 그러나 본 논문에서 제안한 방법은 정상데이터 및 2가지 유형의 공격을 각각 분류하여 탐지할 수 있고, 탐지하는데 소요되는 시간도 기존의 MIB 방법보다 많이 단축되었고, 거의 실시간에 가까운 성능을 보였다.

그림 8은 본 논문에서 제안된 방법을 이용하여 네트워크 트래픽의 정상 데이터와 공격 유형들에 대한 분류 결과를 그래프로 보여준다. 그림 8의 탐지율 DRate은 식 (3)에서와 같이 전체 네트워크 트래픽 실험 데이터 중에서 공격의 유형을 정확하게 인식한 비율을 백분율로 표현한 것을 의미한다.

$$DRate = \frac{correctly\ detected\ attack\ data}{number\ of\ total\ traffic\ data} \times 100 \quad (3)$$

그림 8에서 정상 트래픽 데이터는 공격 트래픽 데이터와 아주 선명한 차이가 있기 때문에 탐지율의 정확도가 매우 높은 편이다.

VI. 결론 및 향후연구

본 논문에서는 네트워크 트래픽 데이터의 헤더파일에서 송신자의 IP와 포트, 그리고 수신자의 IP와 포트 정보를 2차원의 영상으로 시각화한 후 이를 분석하여 이상현상을 효과적으로 분석하는 방법을 제안하였다. 제안된 방법에서는 먼저 송신자와 수신자의 IP 정보를 받아들여 4개의 2차원 영상을 생성하고, 포트 정보를 받아들여 1개의 2차원 영상을 생성한다. 그런 다음, 각 영상 내의 트래픽 데이터를 분석하여 패턴의

특징을 추출하는데, 트래픽의 공격을 나타내는 선형 패턴 또는 높은 명암값을 가지는 패턴을 추출하여 정상 트래픽, DDoS, 그리고 DoS를 자동으로 검출하였다. 실험결과 정상 트래픽과 이상현상 사이의 분류는 잘 수행되었으며, 이상현상 사이의 검출은 오탐지가 일부 발생하였으나 비교적 정확성 있게 수행되었다.

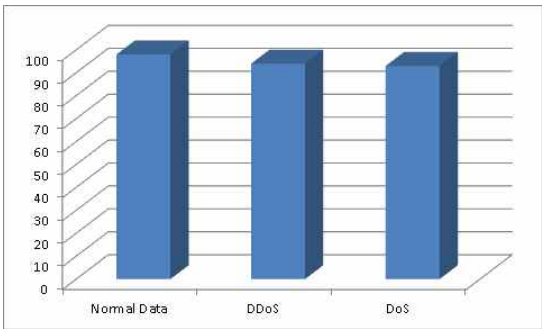


그림 8. 공격 탐지율
Fig. 8. Detection Rate of Attack

향후에는 트래픽 데이터의 시각화 작업 시 보다 정확한 결과를 얻기 위해서 형태(morphological) 연산을 이용하여 잡음제거를 수행할 예정이며, 유사한 트래픽 사이의 군집화를 통해 중간 단계 처리의 효율화를 시도할 예정이다.

참고문헌

[1] S. M. Lee, D. S. Kim, J. H. Lee, and J. S. Park, "Detection of DDoS Attacks Using Optimized Traffic Matrix," Computers and Mathematics with Applications, Vol. 63, No. 2, pp. 501-510, 2012.

[2] E. Corchado and Á. Herrero, "Neural Visualization of Network Traffic Data for Intrusion Detection," Applied Soft Computing, Vol. 11, No. 2, pp. 2042 - 2056, 2011.

[3] M.-T. Kim, Y.-W. Choi, K.-H. Kwon, S.-H. Kim, "Network Attack Detection based on Multiple Entropies," Journal of Korea Institute of Information Security and Cryptology, Vol. 16, No. 1, pp. 71-77, 2006.

[4] S.-H. Park, J.-W. Park, and M.-S. Kim, "Flow-based Real-time Traffic Monitoring and Analysis System," In Proceedings of the Fall Conference of the Korea Information Processing Society, Vol. 14, No. 2, pp. 1061-1064, 2007.

[5] L. P. Gaspary, R. N. Sanchez, D. W. Antunes and E. Meneghetti, "A SNMP-based Platform for Distributed Stateful Intrusion Detection in Enterprise Networks," IEEE Journal on Selected Areas in Communications, Vol. 23, No. 10, pp. 1973-1982, 2005.

[6] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "A Comparative Study of Related Technologies of Intrusion Detection and Prevention Systems," Computers and Security, No. 01, 2012.

[7] Y. Xie and S.-Z. Yu, "Monitoring the Application-Layer DDoS Attacks for Popular Websites," IEEE/ACM Transactions on Networking, Vol. 17, No. 1, pp. 54-65, 2009.

[8] R. Mathew and Vijay Katkar, "Software-based Low Rate DoS Attack Detection Mechanism," International Journal of Computer Applicatiosns," Vol. 20, No. 6, pp. 14-18, 2011.

[9] B. Li, K. Peng, X. Ying, and H. Zha, "Vanishing Point Detection Using Cascaded 1D Hough Transform from Single Images," Pattern Recognition Letters, Vol. 33, No. 1, pp. 1-8, 2012

[10] D.-S. Yoo, H.-O. Koo, C.-S. Oh, "Noxious Traffic Analysis Using SNTP," In Proceedings of the Fall Conference of the Korea Contents Association, Vol. 2, No. 2, pp. 215-219, 2004.

저 자 소 개

장 석 우

2000년 8월: 숭실대학교대학원 컴퓨터학과 (공학박사)

2009년 3월 - 현재: 안양대학교 디지털미디어학과 교수

관심분야 : 로봇비전, 증강현실, HCI, 게임, 비디오 색인 및 검색, 이러닝 등

E-mail : swjang@anyang.ac.kr

김 계 영

1996년 2월 : 숭실대학교대학원 컴퓨터학과 (공학박사)

2001년 3월 - 현재 : 숭실대학교 컴퓨터학과 교수

관심분야 : 컴퓨터 비전, 형태인식, 생체인식, 증강현실, 신호처리 등

E-mail : gykim11@ssu.ac.kr

나 현 숙

2002년 : 포항공과대학교 수학과 (박사)

2003년 3월 - 현재: 숭실대학교 컴퓨터학부 교수

관심분야 : 알고리즘, 계산기하학, 정보이론 등

E-mail : hsnaa@ssu.ac.kr