SOM(Self-Organizing Map)을 이용한 대용량 웹 서비스 DoS 공격 탐지 기법

Detection Mechanism of Attacking Web Service DoS using Self-Organizing Map

이형우, 서종원
한신대학교 컴퓨터공학부

Hyung-Woo Lee(hwlee@hs.ac.kr), Jong-Won Seo(seo0207@lycos.co.kr)

요약

웹 서비스는 개방형 서비스로 정보 공유가 주요 목적이다. 하지만 상대적으로 웹 서비스에 대한 공격 및 해킹 사고 또한 급증하고 있다. 현재 웹 해킹 등의 공격을 탐지하기 위해서는 웹 로그의 분석을 통해 우선적으로 수행 가능하며 중요한 역할을 수행하고 있다. 실제 웹 로그 분석을 통해 웹 서비스의 취약점을 분석하고 보완하는 사례가 늘어나고 있다. 이에 본 연구에서는 대용량의 웹 로그 정보에 대해 SOM 알고리즘을 적용하여 웹 DoS 공격 등과 같은 웹 서비스에서의 이상 탐지를 수행하였다. 구체적으로 대용량 웹 로그 정보에 대해 SOM 기반으로 BMU(Best Matching Unit)의 발생 빈도를 조사해 발생 빈도가 가장 높은 유닛을 이상(Abnormal) 유닛으로 판단하여 입력된 웹 로그 데이터에 대한 DoS 공격 탐지 성능을 향상시킬 수 있었다.

■ 중심어 : | 웹 로그 | 공격 탐지 | SOM |

Abstract

Web-services have originally been devised to share information as open services. In connection with it, hacking incidents have surged. Currently, Web-log analysis plays a crucial clue role in detecting Web-hacking. A growing number of cases are really related to perceiving and improving the weakness of Web-services based on Web-log analysis. Such as this, Web-log analysis plays a central role in finding out problems that Web has. Hence, Our research thesis suggests Web-DoS-hacking detective technique In the process of detecting such problems through SOM algorithm, the emergence frequency of BMU(Best Matching Unit) was studied, assuming the unit with the highest emergence frequency, as abnormal, and the problem- detection technique was recommended through the comparison of what's called BMU as input data.

■ keyword : | Web-Log | Attack Detection | Self-Organizing Map |

I. 서 론

국내의 인터넷 이용률은 꾸준히 증가 추세에 있으며, 현재 국내 인터넷 사용자 수는 약 34,430천명을 넘고 있다. 그리고 2007년 6월 만 6세 이상 인터넷 이용률 (최근 1개월 이내 인터넷 이용자의 비율)은 75.5%이며, 2006년 6월 대비 인터넷 이용률은 73.5%에서 2.0%p 증가, 이용자수는 33,580천명에서 850천명이 증가했다[1].

* 본 연구는 지역대학우수과학자 연구과제(KRF-2007-521-D00467)의 지원으로 수행되었습니다.
* 본 연구의 일부는 지식경제부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었습니다.(IITA-2008-C1090-0801-0016)
접수번호 : #080115-001
접수일자 : 2008년 01월 15일
심사완료일 : 2008년 04월 29일
교신저자 : 이형우, e-mail : hwlee@hs.ac.kr

이처럼 국내 인터넷 이용률 및 이용자 수는 꾸준히 증가 추세에 있으며, 사용자의 연령층 및 직업군 또한 다양해지고 있다.

이처럼 웹 사용자와 웹 서비스의 빠른 증가 추세와 함께 비즈니스 및 많은 사업군이 웹 기반 서비스 방식으로 변화되어 웹 시스템에 대한 기업들의 의존도 또한 높아져 가고 있다. 이처럼 웹 서비스는 다양한 형태로 발전하면서 사용자의 요구사항을 만족시키고 있다.

그와 더불어 다양한 형태의 웹 공격 또한 늘어나고 있는 추세이다. 기존의 웹 이상 탐지 기법은 룰(Rule)에 의한 웹 이상 문자열 탐지 기법(Rule based Anomaly detection)에 그치고 있으며, 이 기법은 대용량화 되고 있는 웹 로그 정보에 대한 효율적 탐지 성능을 보이지 못하고 있다[2][4].

즉, 일반 포털 사이트와 같은 대형 웹 사이트인 경우 W3C 형태의 웹 로그 정보를 생성하도록 웹 서버 관리자에 의해 설정되어 있다. 매일 생성되는 웹 로그 정보의 크기는 대략 수백 MB에서 수 GB에 이르고 있다. 또한 매일 웹 사이트에 접속하는 사용자 수도 수만 개의 트렌젝션 및 세션으로 나눌 수 있을 정도로 방대하다[3]. 따라서 이와 같이 방대한 형태의 웹 사이트에서 생성되는 웹 로그 정보에 대한 분석을 통해 공격을 탐지하기 위해 많은 연구가 진행되었다[4].

대량 웹 로그에 대한 효율적 검색 기능을 제공하기 위한 연구에서부터 웹 로그 내 공격 정보 및 이상 트래픽에 대한 판단을 위한 연구 등 다양한 형태의 연구가 진행되었다[5][6]. 최근 웹 정보를 대상으로 SOM(Self-Organizing Map)[8][9] 알고리즘을 적용하여 그룹화[10][11]하거나 트랜젝션에 대한 판단 및 데이터 마이닝 기술 등에 적용[12], 공격 탐지 등에 접목[13]하기 위한 연구가 진행되었다. 하지만 아직까지 웹 로그 정보를 이용하여 웹 서버에 대한 DoS 공격을 탐지하는 기법에 대한 연구는 수행되지 않았다.

웹 서버에 의해 기록/저장되는 웹 로그 데이터는 상당히 방대한 정보가 생성되며, 웹 이상 현상 등을 바로 추출할 수 없는 형태이다. 따라서 대용량 웹 로그 정보로부터 DoS 공격 등에 대한 시도 등을 판별하고 이를 추출하기 위해서는 효율적인 클러스터링 기법 및 공격 판단 기법이 제시되어야 한다.

SOM 알고리즘은 임의의 입력 데이터에 대해 스스로 자기 조직화하여 이를 내부 벡터 공간으로 사상시켜주는 역할을 수행한다. 따라서 SOM 알고리즘을 웹 로그 데이터에 적용할 경우 n차원의 입력 데이터들을 클러스터링하여 2차원으로 사상시켜주는 기능을 제공할 수 있다. 결국 대용량의 웹 로그내 각 필드로 구성되어 있는 n차원의 데이터 집합에 대해 SOM 알고리즘을 이용하면 DoS 공격 여부를 판단하는 2차원 벡터 값으로 클러스터링하는 기능을 제공할 수 있기 때문에 대용량 웹 로그 정보내 클러스터링 및 웹 이상 탐지 기능에 적용할 수 있다.

따라서 본 논문에서는 웹 로그에 SOM 알고리즘[9]을 적용하여 웹 로그에서 가장 유사 형태의 로그 형태로 그룹 지을 수 있는 로그에 대한 빈도수를 조사하여, 빈도수가 높은 BMU(Best Matching Unit)을 찾고, 발생 빈도가 가장 높은 BMU를 DoS 공격의 패턴으로 판단하는 과정을 수행하여 실제 공격에 대한 탐지율 향상 및 이상 데이터의 비율에 따른 최적화된 SOM 맵 크기 설정 방안 및 구성에 대해 연구하였다.

본 논문의 구성은 다음과 같다. 2장 관련 연구에서는 기존의 웹 이상 탐지 기법을 설명하고 비효율적인 측면에 대해 서술 하였다. 제안 기법 3장에서는 본 논문의 제안 기법에 대해 설명하고, 4장에서는 실험 결과에 대해 언급했다. 마지막 장에서는 결론 및 향후 연구 방향에 대해 제시하였다.

II. 관련연구

1. 기존 웹 이상 탐지 기법의 비효율성

기존에 스노트(snort)와 같은 네트워크 기반의 침입탐지 시스템은 웹 응용 프로그램의 보안 시스템으로 적합하지 않다. 그 문제는 수많은 오용탐지 및 웹 트래픽의 상관관계에 대한 분석이 취약하다는 점이다. 그리고 웹 서버가 SSL(Secure Sockets Layer) 상에 존재한다면 침입탐지 시스템은 무용지물이다. 그러므로 기존의 웹 이상탐지 기법은 호스트 기반의 룰을 통한 이상 문

자열 탐지 기법을 사용하고 있다[2].

웹 로그는 특정 필드 값들의 배열로 이루어졌으며, 이 특정 값들은 사용자의 송수신 정보를 담고 있다. 그러므로 웹 로그의 문자열들은 기존의 공격 로그와 비교하여 이상탐지기법에 적용하고 있다. 예를 들어 아래의 웹 로그는 해커들이 웹 공격 이전에 웹 시스템의 취약점 정보를 얻기 위한 웹 스캔 과정의 공격 패턴이다.

```
100.149.117.1 - - [13/Jan/2006:01:03:30 -0200]
"POST /blog/xmlrpc.php HTTP/1.0" 404 288
100.149.117.1 - - [13/Jan/2006:01:03:31 -0200]
"POST /blog/xmlsrv/xmlrpc.php HTTP/1.0" 404 295
100.149.117.1 - - [13/Jan/2006:01:03:32 -0200]
"POST /blogs/xmlsrv/xmlrpc.php HTTP/1.0" 404 296
100.149.117.1 - - [13/Jan/2006:01:03:33 -0200]
"POST /drupal/xmlrpc.php HTTP/1.0" 404 290
100.149.117.1 - - [13/Jan/2006:01:03:35 -0200]
"POST /phpgroupware/xmlrpc.php HTTP/1.0" 404 296
100.149.117.1 - - [13/Jan/2006:01:03:36 -0200]
"POST /wordpress/xmlrpc.php HTTP/1.0" 404 293
100.149.117.1 - - [13/Jan/2006:01:03:44 -0200]
"POST /xmlrpc/xmlrpc.php HTTP/1.0" 404 290
100.149.117.1 - - [13/Jan/2006:01:03:46 -0200]
"POST /xmlsrv/xmlrpc.php HTTP/1.o
```

이 웹 로그는 100.149.117.1이라는 사용자가 13/Jan/2006: 01:03:30 ~ 13/Jan/2006: 01:03:46초 동안 POST방식의 웹 요청 사항을 보여주고 있다. 이것은 일정한 시간동안 동일한 사용자로부터 연속적인 요청을 받을 시 그리고 서버의 상태 코드가 404(Not Found[3]) 이라는 상태일 때 이것을 웹 스캔으로 정의했다. 이 기법은 웹 로그의 문자열들의 검색 기능으로 구현하였으며, 쿼리 문에 대한 룰 검색을 통해 SQL Injection, Parameter Injection등의 입력 값 검증 부재로 인한 공격 또한 탐지가 가능하다.

[그림 1]은 SQL Injection, Common Web Attack에 대한 XML 형태의 룰 파일이다. 웹 로그 문자열에서 정의된 룰 문자열을 탐색해 출현하면 공격 로그로 판단하는 방식으로 웹 이상탐지가 이루어진다.

```
<description>SQL injection attempt.</description>
<group>attack,sql_injection,</group>
</rule>
- <rule id="31104" level="6">
<if_sid>31100</if_sid>
- <!--
Attempt to do directory transversal, simple sql injections,
- or access to the etc or bin directory (unix).
-->
<url>%027|%00|%7f|%2E%2E|%0A|%0D|../..|..\..|echo;|..</url>
<url>cmd.exe|root.exe|_mem_bin|msadc|/winnt/|</url>
<url>/x90/|default.ida|/sumthin|nsiislog.dll|chmod%|wget%|cd%|</url>
<url>cat%|exec%|rm%20</url>
<description>Common web attack.</description>
<info>http://www.armbrustconsulting.com/LogEntries.html</info>
<group>attack,</group>
</rule>
- <rule id="31105" level="6">
<if_sid>31100</if_sid>
<url>%3Cscript|%2Fscript|script>|script%3E|SRC=javascript|IMG%20|</url>
<url>%20ONLOAD=|INPUT%20</url>
<description>XSS (Cross Site Scripting) attempt.</description>
<group>attack,</group>
</rule>
- <rule id="31106" level="12">
<if_sid>31103, 31104, 31105</if_sid>
<id>^200</id>
<description>A web attack returned code 200 (success).</description>
<group>attack,</group>
</rule>
```

그림 1. 웹 이상 탐지 룰

룰 기반의 탐지 시스템이 가지고 있는 새로운 공격에 대한 탐지 불능[4]의 취약점, 높은 False Positive Rate[5], 하나의 입력 데이터에 의한 공격 탐지가 아닌 데이터들의 상호 연관관계에 의한 공격 탐지 기법 등의 적용이 취약하다는 문제점을 보이고 있다.

그러므로 본 논문은 웹 로그 필드 단위의 문자열 특성을 고려한 인덱스 기법 및 B-트리 구조를 이용해 웹 로그 공격탐지 시 문자열의 탐색 성능을 높였다. 그리고 단일 로그에 대한 룰 비교 공격탐지 기법의 취약점을 보완하기 위해 웹 로그의 SOM (Self-Organizing Map) 알고리즘을 적용하였다. 그러므로 웹 로그의 상호 연관성을 고려한 정상과 비정상 로그의 분류가 가능하였다. SOM 설정 과정은 다음과 같다.

2. SOM(Self-Organizing Map)

연결 가중치벡터들의 초기값은 임의의 값으로 할당하며, 입력벡터와 유사성을 측정한다. 유사성 측정의 방법은 유클리드거리(Euclidean Distance)를 많이 사용한다. 입력벡터와 k개의 Fan-in weight vector 사이의 유클리드 거리를 구하여 입력벡터와 가장 유사한(유클리드 거리가 가장 작은) j번째 Fan-in weight vector를 찾으면 그 입력 벡터에 대한 j번째 출력 노드가 승자(BMU)가 된다. 이렇게 승자를 선택하면 승자의 Fan-in weight vector는 갱신되게 된다.

Algorithm SOM
Input : Set of N dimension vector, X
Output : Subset of input data (M subsets)

```
begin
    Randomly initialize Wi = (wi1, wi2,....,win) for each node
    for ( t=0; unless a stopping condition is reached;
          Increase t)
        for (for all input data)
            for ( i=0 to M)
                Compute Di=||Xt-Wi(t)||
            endfor
            Find the winner j=i such that Dj(t) is minimum
                for over all i
            Update the winner j (and its neighbors)
        endfor
    endfor
end
```

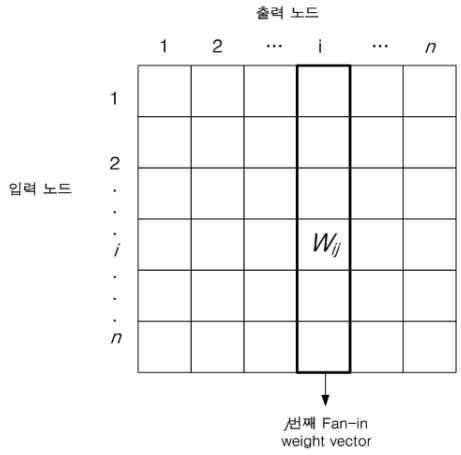


그림 2. 연결 가중치 행렬

연결 가중치 벡터 갱신과정은 Normalized Vector Sum, Vector Difference 기법이 있다. 두 가지 기법의 차이는 있지만 가중치 벡터가 입력 벡터방향으로 이동하는 공통점을 가지고 있다. 연결 가중치 벡터를 갱신하는 경우, 승자(Winner)가 된 노드의 Fan-in weight vector만 갱신하지 않고 그 노드의 이웃 노드들의 연결 가중치도 갱신하는 기법을 사용하고 있다.

이웃 노드를 결정할 때는 4-연결성 또는 8-연결성의 노드로 결정된 것이고, 이때 어떤 입력 벡터에 대한 승자 노드가 6번이라면, 4-연결성에 의해서는 2, 5, 7, 10이 이웃 노드가 될 것이고, 8-연결성에 의해서는 1, 2, 3, 5, 7, 9, 10, 11이 이웃노드가 될 것이다. 즉, 어떤 입력 벡터의 승자노드가 6번이라면, 다음 3가지 중 하나의 방법을 사용하여 가중치 벡터를 갱신할 수 있다.

- 6번 노드의 가중치 벡터만 갱신한다.
- 6, 2, 5, 7번 노드의 가중치 벡터를 갱신한다.(4-연결성 이웃노드)
- 6, 1, 2, 3, 5, 7, 9, 10, 11번 노드의 가중치 벡터를 갱신한다.(8-연결성 이웃노드)

가중치 벡터의 갱신을 위해서 사용하는 함수는 아래 수식이다.

$$w^j(t+1) = w^j(t) + \alpha(t)[x(t) - w^j(t)]$$

$$\alpha(t) = 0.1(1 - t/10^k), \text{단} k\text{는상수}$$

가중치 벡터 갱신 함수에 따라 각 출력노드의 가중치 벡터는 그 출력노드에 포함된(그 출력노드를 승자로 선택함) 입력 데이터 방향으로 이동한다. 그 움직임은 초기에는 산만하나, 입력벡터의 수가 어느 정도 이상이 되면 거의 변화하지 않고 안정된다. 학습이 끝난 후 각각의 Fan-in weight vector는 각 분류 영역의 중심에 근사한다. 충분히 학습된 SOM은 임의의 입력을 분류하여 특정 클래스에 할당할 수 있다. 학습 단계에서 사용된 데이터와 유사한 데이터가 입력으로 들어오면 맵 상에서 가장 유사한 노드가 승자가 되고 해당 노드로 분류되며, 전혀 새로운 데이터가 입력으로 들어오면 맵에서 비슷한 클러스터가 없으므로 새로운 노드가 할당되어 새 클러스터를 만들게 된다.

III. 제안 기법

제안한 DoS 공격탐지 알고리즘은 3단계로 이우러 진다. 첫째는 웹 로그를 수집해 공격 탐지를 위한 Feature Selection 작업 및 전처리 단계, 두 번째는 탐지에 필요한 맵을 생성하는 학습 단계, 마지막 단계는 DoS 공격 탐지 단계이다.

먼저 탐지 대상이 되는 웹 로그의 수집이 선행 되어

야 한다. 그리고 이상 탐지에 적합한 로그 필드의 추출 및 전처리 과정이 필요하다. 또한 정상과 이상 로그로 분류하기 위한 맵인 U-matrix를 생성하는 단계에서는 어느 특정 속성 값의 차이에 따른 전체 맵의 변화를 최소화하기 위해서 정규화(normalization) 과정을 수행한다. 그리고 맵의 각 뉴런 값을 초기화 시킨 후 입력된 로그 데이터의 클러스터들을 대표할 수 있는 뉴런인 BMU(Best Matching Unit)을 선택하고 그 이웃 뉴런 값을 갱신한다. 입력 데이터가 모두 학습될 때까지 이 과정을 반복하면 학습 단계가 끝나게 된다.

이때 DoS공격의 특성상 특정 시간동안 많은 양의 로그가 쌓이고 이 로그들의 BMU 값은 유사한 형태를 보이고 있다. 그러므로 빈도수가 가장 높은 BMU를 공격 로그로 간주하고 입력 데이터에 대한 BMU 값과의 비교로 이상 여부를 판단한다. 구체적인 판단 과정을 도식화하면 다음 그림과 같다.

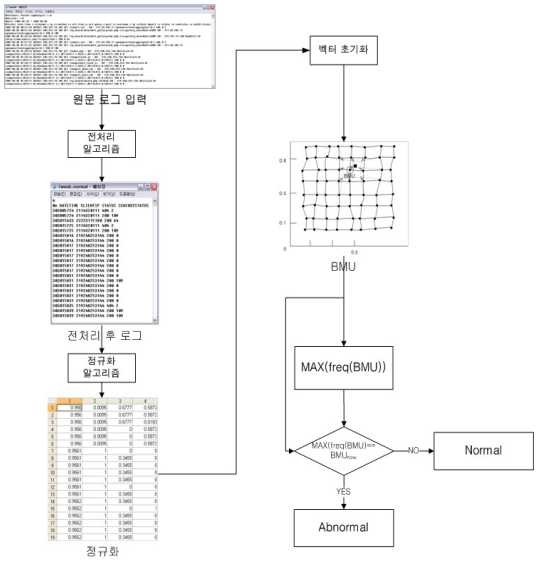


그림 3. 제안 알고리즘 흐름도

1. 웹 이상 탐지를 위한 특징값 추출

웹 로그를 이용한 DoS 공격탐지를 위해서는 일부 필드들의 복합적인 연간 관계를 고려해 특정 필드의 정보를 추출하여 웹 로그 패턴을 분류해야 한다. 이때 분류되는 패턴을 정상(Normal)과 비정상(Abnormal)으로 분류 한다. 일반적으로 웹 로그 정보에 대해 이상행위를 탐지하기 위해 사용하는 필드 정보를 다음 [표 1]과 같다. 이는 기존 연구[6]에서도 동일하게 사용한 것이다.

이처럼 웹 로그를 통한 웹 이상탐지 기법을 적용하기 위해서는 특정 공격에 적합한 로그 필드 요소 추출이 선행 되어야 한다. 앞 절에서 uri-stem, uri-query 필드들은 고속전처리를 이용한 특수 문자열 검색으로 웹 이상을 탐지하는 기법에 사용했다. 그러므로 DoS 공격탐지를 위해 로그의 시간적 주기 및 특정 사용자의 식별, 서버의 상태를 고려해 본 논문에서는 웹 로그의 c-ip (클라이언트 IP주소), date-time(로그 발생 날짜와 시간 정보), sc-status(서버의 action 상태정보), sc-win32-status(서버 OS의 action 상태정보)필드들을 추출해 분석 대상이 되는 로그들 간의 상관관계를 고려했다.

표 1. IIS 6.0 각 필드별 이상 행위 고려사항

Field	Description
c-ip	한 IP에서 많이 요청되었는가?
	사용된 IP가 정상 등록된 IP인가?
date-time	특정시간에 집중되었는가?
	주기적으로 요청되었는가?
cs(user-agent)	한 IP에서 UA의 종류가 많은가?
cs-uri-stem	특정 페이지만을 집중적으로 요청했나?
	요청된 페이지가 대중적인가?
	요청된 페이지에 취약성이 존재하는가?
cs-uri-query	요청된 쿼리에 취약성 공격이 있는가?
sc-status	특정 에러 코드에 집중되는가?
time-taken	처리시간의 편차가 심한가?
cs-byte	전송 byte의 편차가 심한가?
cs(referer_)	정상적인 Referer에서 요청되었는가?

2. 대용량 웹 로그 전처리 모듈

웹 로그의 필드 중 학습과정의 입력 데이터로 활용할 필드의 추출 및 통합 과정을 전처리라 한다. 웹 로그는 특정 형식을 가지고 있으며, 웹 시스템 관리자에 따라 웹 로그 필드의 구성이 상이할 수 있다. 그러므로 본 논문에서는 DoS공격 탐지에 효과적인 앞 절에서 추출한 date, time, c-ip, sc-status, sc-win32-status필드의 정보를 사용하여 전처리 과정을 수행하였다.

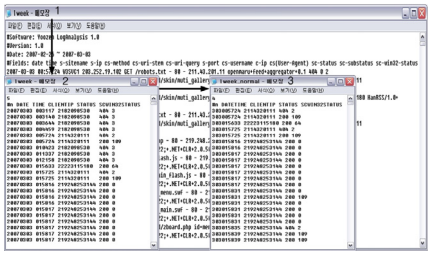


그림 4. 웹 로그 전처리

또한 추출한 필드 중 date와 time필드를 연접시키고 년도는 삭제 하였다. 그 이유는 전체 웹 로그에서 연월일의 차이가 빈번하게 일어나지 않으며, 시간에 따른 웹 로그의 차이를 적용시키기 위함이다.

아래 [표 2]는 본 논문에서 사용한 필드별 값의 범위를 보여주고 있다. date필드의 값이 2007-03-04일 경우 20070304로 표현했으며, client ip의 값이 192.168.100.100일 경우 192168100100으로 표현했다. sc-status 및 sc-win32-status의 경우 실제 코드 값을 사용하였다. 그러나 앞서 언급했듯이 실제 입력은 4가지 속성을 사용하였고 date필드와 time필드를 통합하여 date필드의 년도 정보를 삭제하였다.

즉, 대용량의 웹 로그 정보에서 생성되는 로그 정보를 SOM 알고리즘에 적용하기 위해 W3C IIS 웹 로그에 기록된 각각의 필드에 대해 DoS 공격과 관련되는 필드를 중심으로 정규화 과정을 수행하고 이를 토대로 DoS 공격에 대한 판별 및 이상 탐지 과정을 수행하게 된다. 공격 탐지를 위한 웹 로그 필드 구성은 다음과 같다.

표 2. 공격 탐지를 위한 웹 로그 필드 구성

Index	Feature	Type Value	Scope
1	date	real	yyyymmdd
2	time	real	hhmmss
3	client ip	real	0000~255255255255
4	sc-status	real	100~505
5	sc-win32-status	real	-

3. 웹 이상 탐지를 위한 정규화 모듈

SOM에서는 각 필드 속성 맵들의 형태를 결합하여 모든 필드 속성이 고려된 U-matrix를 분류 결과로 도출한다. 그러나 각 필드의 속성 값들은 다양한 범위의 값을 갖는다. 예를 들어 sc-status 코드는 100~505의 범위를, client ip는 0000~255255255255의 범위를 갖는다. 그러므로 client ip 속성 값의 변화는 sc-status 속성 값의 변화 보다 U-matrix에 더 큰 영향력을 끼치게 된다. 정규화 과정을 거치지 않은 U-matrix는 범위의 차이가 큰 속성 값에 의해 맵을 형성하는 문제를 야기 시킨다.

본 논문의 정규화 과정은 각 필드 속성 값을 최소값 0으로($V_{\min}(x) \Rightarrow 0$), 최대값을 ($V_{\max}(x) \Rightarrow 1$) 변형한 아래 수식을 사용하여 모든 값이 일정한 범위인 0~1로 구성하도록 정규화 한다.

$$N_{i(x)} = (i(x) - V_{\min}(x)) / (V_{\max}(x) - V_{\min}(x))$$

[그림 5]와 [그림 6]을 통해 정규화 하지 않은 U-matrix와 정규화한 U-matrix를 비교 할 수 있다. 모든 필드 속성을 정규화한 그림 6의 U-matrix는 각 속성 값의 고른 영향을 받아 분류된 것을 볼 수 있다. 그러므로 각 속성 값의 차이가 잘 적용된 통합된 분류 결과(U-matrix)를 얻을 수 있었다.

그러나 정규화 과정을 거치지 않은 [그림 5]의 U-matrix는 속성 값의 편차가 심한 client ip에 의해 맵이 형성되어 client ip 필드의 속성 값이 입력 로그 분류 과정에 가장 많은 영향을 준다는 것을 알 수 있었다. 따라서 웹 로그 정보에 대해서 정규화 과정을 수행하여 DoS 공격 탐지 과정을 적용해야 한다.

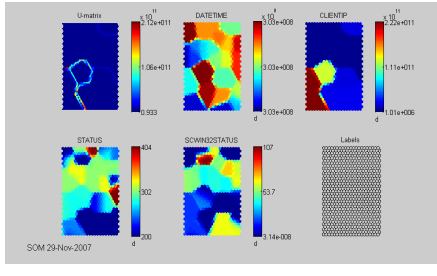


그림 5. 비정규화 결과

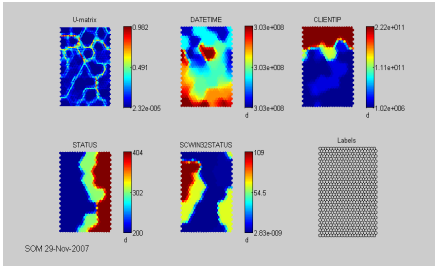


그림 6. 정규화 결과

4. SOM 알고리즘을 이용한 학습 모듈

SOM(Self-Organizing Map)은 신경망 기법을 사용하는 클러스터링 모델이다. SOM의 특징은 비지도 학습 기법을 사용하므로 침입탐지에 있어서 미리 정의된 정상과 비정상의 학습데이터가 필요하지 않고, 분류되지 않은 학습 데이터를 입력하면 유사한 속성의 데이터끼리의 클러스터링을 통해 기계 스스로가 정상과 비정상 트래픽으로 분류해준다.

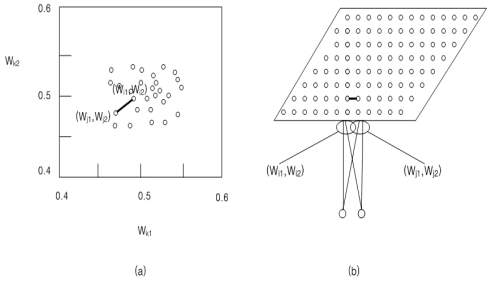


그림 7. 초기 연결강도 및 경쟁층에서 인접 유닛의 연결

[그림 7]의 예를 통해 SOM 알고리즘이 어떻게 2차원 지도에 자기조직화를 하는지 알 수 있다[7].

SOM은 [그림 7]의 (a)에 나타난 것처럼 처음의 상태에서 점차 조직화된다. 그러므로 최종적으로 [그림 8]의 연결강도를 가진 맵을 조직한다. [그림 8]은 입력 패턴에 대한 맵의 반응 원리를 보여주고 있다.

본 논문에서 사용한 입력은 특정 필드의 속성 값으로, SOM 알고리즘을 사용해 입력 패턴에 대한 반복적인 맵의 반응으로 U-matrix가 형성되었으며 [그림 8]의 밝은 색은 이웃 클러스터와 구분 지어주는 경계선을 의미한다. Labels는 BMU(Best Matching Unit)을 레이블링한 결과로 BMU의 맵 위치와 U-matrix의 어두운 부분의 중심부와 일치하는 것을 볼 수 있다. 즉 입력 데이터에 대한 연결 가중치 벡터의 갱신으로 클러스트 된 결과라 볼 수 있다.

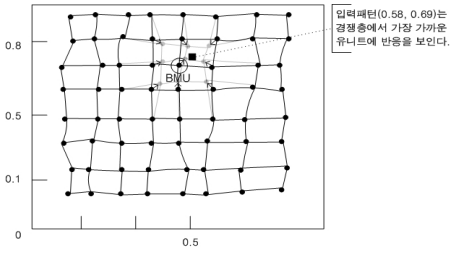


그림 8. 주어진 입력패턴에 대한 맵의 반응

이 결과는 본 대학내 주요 홈페이지의 1주일(ex070226~ex070303)[1] 동안의 IIS 6.0 웹 로그 중에서 300 라인만을 추출한 것이며, [35 21]의 맵 사이즈에 사상시켜 얻은 것이다. 이때 [a,b] 값은 BMU의 [세로축 셀의 개수, 가로축 셀의 개수]를 의미한다.

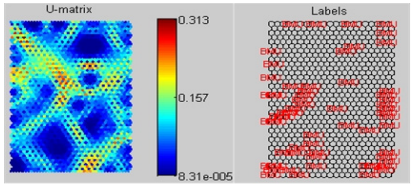


그림 9. U-matrix와 BMU(Best Matching Unit)

5. SOM 기반 웹 로그 DoS 공격 탐지

SOM을 이용한 DoS공격 탐지 기법은 다음과 같은 순서에 의해 진행 된다. 첫째, 정상 데이터와 비정상 데이터가 섞여있는 로그의 학습과정을 거쳐 맵의 뉴런 중 최소거리를 갖는 승자뉴런인 BMU 값을 추출한다. 둘째, 추출한 BMU 값들의 빈도수를 고려해 가장 높은 빈도수의 BMU 값을 공격 클러스터의 BMU로 가정한다. 셋째, 입력 데이터에 대한 BMU 값과의 빈도수가 가장

1 로그 파일명은 ex연월일 형식으로 웹 서버에 의해 자동으로 생성되도록 하였음

많았던 BMU 값과의 비교 과정을 거쳐 이상을 탐지 한다. BMU가 정상 클러스터이면 입력 데이터는 정상 로그, 비정상 클러스터이면 입력 데이터는 비정상 로그로 정의한다.

Algorithm Abnormal Detection
Input : $x(n)$
Output : Detection Result
MBMU=MAX(freq(BMUS))
if BMU of $x(n)$ == MBMU
then $x(n)$ = abnormal
else $x(n)$ = normal

IV. 성능 분석 및 평가

1. 제안한 기법의 성능 평가 및 분석

본 성능 분석 및 평가는 맵 사이즈 및 로그 사이즈에 따른 탐지 결과를 비교 분석 한다. 본 논문의 이상 탐지 실험을 위해 그림 2의 탐지 알고리즘을 이용 했으며 구현은 MATLAB의 SOM Toolbox[8]를 이용하여 웹 로그 이상 탐지에 적합한 형태로 수정 및 보완 하였다.

이상탐지 결과 및 분석의 기본적인 탐지 성능 평가 항목으로 탐지율, False Positive, False Negative를 측정 했다.

실험 대상인 데이터는 웹 서버로부터 생성된 W3C IIS 포맷 형태의 웹 로그 정보를 사용하였으며, 웹 로그 정보에서 랜덤하게 로그 정보를 일정 부분에서 추출하여 SOM 학습 자료로 사용하였다. 특히 실험의 정형화를 위해 SOM 학습에 사용하는 이상 로그는 500 라인으로 설정하였다. 맵 사이즈는 입력데이터의 출력 맵으로 맵의 크기의 변화에 따른 분류 성능을 알아볼 수 있었다. 아래 표는 웹 로그 및 맵 사이즈에 따른 DoS 공격 탐지율에 대한 실험 결과이다.

맵 사이즈가 작은 경우 입력 데이터에 동일한 BMU 값을 갖는 Log Line이 증가한다. 그러므로 적은 수의 BMU로 입력 데이터가 일반화 된다. 즉 입력 데이터의 적절한 맵 사이즈 설정을 통해 분류가 이루어 져야 정확한 탐지가 가능하다. 본 논문의 실험 결과에 따르면, 맵 사이즈와 탐지율은 비례관계에 있다는 것을 알 수 있었다.

표 3. 로그 및 맵 사이즈에 따른 탐지율(%)

Log size / Map size	5000 (Line)	10000 (Line)	15000 (Line)	20000 (Line)
[5 3]	0.2	0.2	0	0
[10 6]	99.6	0.2	0	0
[20 12]	99.6	99.8	0	0
[30 18]	99.6	99.8	99.8	0
[40 24]	99.8	99.8	99.8	100
[50 30]	99.8	99.8	99.8	100

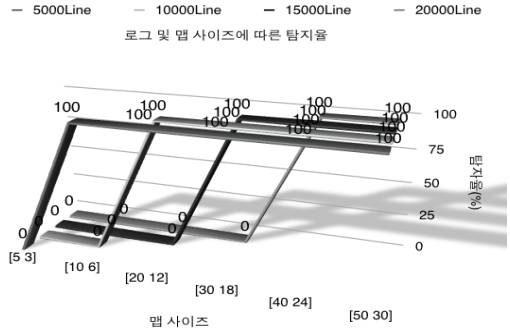


그림 10. 로그 및 맵 사이즈에 따른 탐지율(%) 그래프

표 4. 로그 및 맵 사이즈에 따른 False Positive(%)

Log size / Map size	5000 (Line)	10000 (Line)	15000 (Line)	20000 (Line)
[5 3]	27.06	29.11	25.96	25.16
[10 6]	6.8	22.46	14.05	13.04
[20 12]	0.46	3.73	6.79	7.73
[30 18]	0.28	0.47	1.23	3.65
[40 24]	0.06	0.56	1.17	0.64
[50 30]	0.04	0.33	0.37	0.31

5,000 라인, 10,000 라인 및 15,000, 20,000 라인에 해당하는 웹 로그 정보에 대해 각각 다양한 형태의 BMU 맵 크기를 설정하여 DoS 공격에 대한 이상탐지 성능 분석 과정을 수행하였으며, 위 [표 4]와 같이 False Positive 성능에 대해 측정해 보았다.

측정 결과 BMU 맵 크기가 클 경우 DoS 공격에 대한 False Positive 값이 낮아지는 것을 알 수 있었으며, 점차적으로 탐지 성능이 높아지는 것을 볼 수 있었다.

침입 탐지 시스템에서 False Positive의 수치는 중요한 성능평가 항목이다. 전체 정상 데이터에서 비정상으로 오판한 데이터의 비율을 나타내는 수치로 False Positive와 맵 사이즈는 반비례의 관계를 가지고 있다는 것을 알 수 있었다.

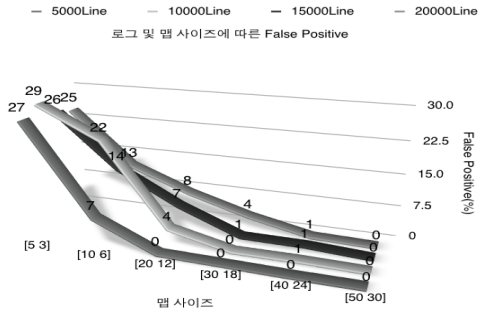


그림 11. 로그 및 맵 사이즈에 따른 False Positive(%)그래프

표 5. 웹 로그 및 맵 사이즈에 따른 False Negative(%)

Log size / Map size	5000 (Line)	10000 (Line)	15000 (Line)	20000 (Line)
[5 3]	99.8	99.8	99.8	100
[10 6]	0.4	99.8	100	100
[20 12]	0.4	0.2	100	100
[30 18]	0.4	0.2	0.2	100
[40 24]	0.2	0.2	0.2	0
[50 30]	0.2	0.2	0.2	0

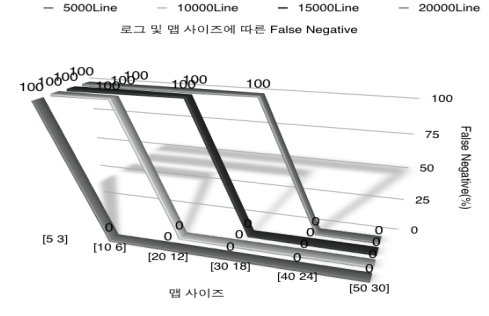


그림 12. 로그 및 맵 사이즈에 따른 False Negative(%) 그래프

False Negative는 전체 데이터에서 정상으로 오판된 비정상 데이터로 맵 사이즈가 커지면 커질수록 False Negative는 줄어들게 된다.

2. SOM 맵 구성 방안

본 논문의 연구 결과 SOM 알고리즘을 이용한 대용량의 웹 로그에서 효과적인 이상탐지를 위해서는 입력 데이터가 사상되는 맵 사이즈의 설정이 탐지 성능에 큰 영향을 미치고 있었다. 탐지 알고리즘에서 맵 사이즈의 크기를 확대 시키면 입력 데이터들을 다양한 맵 유닛에 표현할 수 있었다. 또한 정상로그에 대한 이상 로그의 비율(각 로그에 따라 1/10. 1/20, 1/30, 1/40의 이상 데이터 구성)이 반비례하도록 맵 사이즈를 결정해야 높은 탐지율과 낮은 False Positive 및 False Negative를 유지할 수 있었다.

그러므로 본 논문에서는 아래의 일반화된 맵사이즈의 최적화 수식을 아래와 같이 제안할 수 있었다. 여기서 k는 맵 사이즈의 비율을 의미하는 상수이며 웹 서버 시스템 환경에 따라 설정하게 된다.

$$Mapsize(n) = k \times 4(\frac{n}{10})^2$$

V. 결론

현재 웹 환경은 다양한 웹 서비스의 발달로 사용자가 급증하고 그에 따른 웹 해킹 사고 또한 증가하고 있다. 그에 대한 대책으로 기존에 웹 로그의 통계적 분석 기법을 이용해 웹 로그를 분석 하였다. 그리고 이상 문자열의 순차적인 탐지 기법을 이용하였다. 그러나 이 같은 기법들은 단일 웹 로그에 대한 단순한 비교에 그치고 있었다.

본 논문에서는 대용량의 웹 로그를 전처리하여 효율적 검색 및 이상탐지 기능을 수행할 수 있는 형태로 정규화 하였으며, SOM 알고리즘을 적용하여 BMU 값의 빈도수를 측정하였고, 그 결과 웹 로그 정보내 DoS 공격에 해당하는 BMU를 탐지/분류할 수 있었다. 성능 분석 결과 SOM 맵 사이즈에 따른 탐지 성능의 차이를 보였다. 또한 본 논문에서는 이상 로그의 비율에 따른 최

적 맵 사이즈 설정 공식을 도출하여 웹 로그 정보내 DoS 공격 탐지 등에 적용 가능하였다.

참 고 문 헌

[1] 정보통신부 한국인터넷진흥원, “2007년 상반기 정보화 실태조사 요약보고서,” 2007.

[2] http://www.ossec.net/en/loganalysis.html

[3] R. Fielding, J. Gettys, J. C. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. L. Berners, Network Working Group, Request for Comments 2616, “Hypertext Transfer Protocol - HTTP/1.1,” pp.45, 1999(6).

[4] K. Christopher, V. Giovanni, "Anomaly Detection of Web-based Attacks," CCS'03, Washington, DC, USA, pp.27-31, 2003(10).

[5] 이준섭, 김상록, 이민수, 조상현, 차성덕, 한국과학기술원(KAIST) 전산학과, "대용량 웹 로그에서의 규칙 기반 침입 탐지 시스템 적용의 방법과 한계성", 한국정보보호학회 하계 학술대회 CISC, Vol.17, 2007(8).

[6] 김상록, 이민수, 이준섭, 조상현, 차성덕, 한국과학기술원(KAIST) 전산학과, "대용량 웹 로그 대상 이상탐지를 위한 이상 특성 추출", 한국정보보호학회 하계 학술대회 CISC, Vol.17, 2007(8).

[7] J. E. Dayhoff, "Neural Network Architectures - An Introduction," Van Nostrand Reinhold, New Yock, 1990.

[8] V. Juha, H. Jonhan, A. Esa, and P. Juha, "SOM Toolbox for Matlab 5," SOM Toolbox Team Helsinki University of Technology, 2000(4).

[9] T. Kohonen, E. Oja, O. Simula, A. Visa, and J. Kangas, "Engineering applications of the self-organizing map," Proceedings of the IEEE, Vol.84, No.10, pp.1358-1384, 1996.

[10] C. Y. Christopher, C. Hsinchun, and H. Kay, "Exploring the World Wide Web with Self-Organizing Map," WWW conference, 2002.

[11] A. S. Kata, N. Alan, "Web page clustering using a self-organizing map of user navigation patterns," Special Issue, Web data mining, Vol.35, No.2, pp.245-256, 2003.

[12] D. Chen, J. C. Patra, and C. P. Fu, "Personalized Web search with self-organizing map," e-Technology, e-Commerce and e-Service, IEEE APOS'05. Proceedings, pp.144-147, 2005.

[13] L. L. DeLooze, "Attack Characterization and Intrusion Detection using an Ensemble of Self-Organizing Maps," Information Assurance Workshop, pp.108-115, 2006.

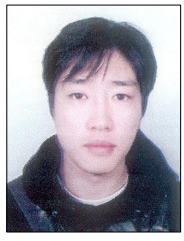
저 자 소 개

이 형 우(Hyung-Woo Lee) 정회원

- 1994년 2월 : 고려대학교 컴퓨터학과(이학학사)
- 1996년 2월 : 고려대학교 컴퓨터학과(이학석사)
- 1999년 2월 : 고려대학교 컴퓨터학과(이학박사)
- 1999년 3월 ~ 2003년 2월 : 백석대학교 정보통신학부 교수
- 2003년 3월 ~ 현재 : 한신대학교 컴퓨터공학부 교수

<관심분야> : 정보보호, 네트워크보안, 무선랜, 침입탐지/차단, 웹 보안 기술, 컨텐츠 보호

서 종 원(Jong-Won Seo) 정회원



- 2006년 2월 : 백석대학교 정보통신학부(공학사)
- 2008년 2월 : 한신대학교 컴퓨터정보학(이학석사)
- 2008년 3월 ~ 현재 : (주)토필드 연구소 연구원

<관심분야> : 정보보호, 네트워크보안, 무선랜, 침입탐지/차단, 웹 보안 기술