기계학습을 이용한 방화벽 로그분석에 관한 연구

김대중
고려대학교 컴퓨터정보통신대학원 미디어공학과
e-mail:aireagle@naver.com

Research Regarding the Fire-Wall log Analysis which users Machine Learning

Dae-Jung Kim
Dept. of Media Engineering.
Gradute School of Computer Infomation and Communications,
Korea University

요 약

인터넷 사용의 증가 및 정보보호에 대한 의식의 증가로 인하여 누가, 언제, 어떻게 해당 사이트를 이용 하였는가 뿐만 아니라 어떤 침해 사고를 일으키고 있느냐에 대한 이슈도 증가하고 있다. 따라서 본 논문에서는 방화벽 원시로그를 기계학습기법을 이용하여 보다 빠르게 방화벽 원시로그의 침해사고에 대한 지능형 모델을 제안한다.

1. 서론

최근 각 기업에서는 해당 기업의 데이터 및 고객의 데이터를 보호하기위하여 방화벽 설치가 늘어나고 있는 추세이다. 설치된 방화벽에는 기존의 침해사례를 통해 나타난 특정 port 및 유해사이트, 공격패턴 등의 정보를 관리자가 미리 정의해 둠에 따라 불법 사용자의 접근을 미리 차단하는 방법으로 방화벽의 구성이 이루어져 있다. 하지만 인터넷의 빠른 확산으로 보다 지능적이고 강도 높은 침해사례가 발생하고 있다.

본 논문에서는 방화벽 원시로그를 기계학습기법을 이용해 제안 모델을 설계하고 구현 과정에 대해 설명하고, 본 연구의 결론과 향후 과제에 대해 기술한다.

2. 관련연구

분류작업을 자동으로 수행하는 사례는 여러 가지가 있는데, 그 중 대표적인 분류 대상으로는 전자우편, 뉴스기사, 엔터테인먼트 선별 등이 있다. 다음은 분류대상에 따른 사례이다.

2.1 Maxims

전자우편을 분류하는 시스템은 Maxims(Laskari, Metral, and Maes 1994)이다[1]. 이 시스템은 메모리 기반의 학습 알고리즘을 사용하여 개발 되었으며, 사용자 전자우편에 대하여 순위결정, 삭제, 정렬, 기록을 수행하여 전자우편을 관리하는 에이전트이다. 이 에이전트는 평소 사용자가 전자우편을 받았을 때 행동하는 모습을 학습의 자료로 사용하기 위해 메모리에 저장하였다가, 비슷한 상황이 발생하였을 때 사용자의 행동에 조언을 하는 시스템이다.

2.2 NewT

인터넷의 발전으로 수많은 정보가 네트워크로 들어오는 가운데 뉴스분야의 정보는 계속적인 스트림(stream)의 형태로 네트워크상으로 유입 된다. 이러한 뉴스의 스트림 가운데 사용자가 원하는 기사의 선택을 위한 시스템으로 NewT가 있다[1]. NewT는 뉴스의 기사를 정치, 경제, 컴퓨터, 스포츠 4가지 클레스로 필터링 한다. 뉴스기사 문서 분석은 백터-공간 모델을 사용한 풀-텍스트 분석으로 이루어지며, 사용자는 충분히 학습된 에이전트를 복사하여 다른 사용자에게 제공할 수 있도록 유닉스환경의 C++로 구현되었다.

2.3 Ringo

분류 시스템의 응용프로그램 중에서 엔터테인먼트 선별을 위한 시스템으로 Ringo가 있다[1]. 엔터테인먼트 선별은 어떤 다른 분류 대상 보다 앞으로 가장 핵심이 되는 대상이 될 가능성이 높은 에이전트 시스템이다. Ringo는 개인을 대상으로 구성된 음악추천시스템(Standanand and Naes 1995)으로 유닉스 환경에서 perl 언어로 구현되었다.

3. 제안모델

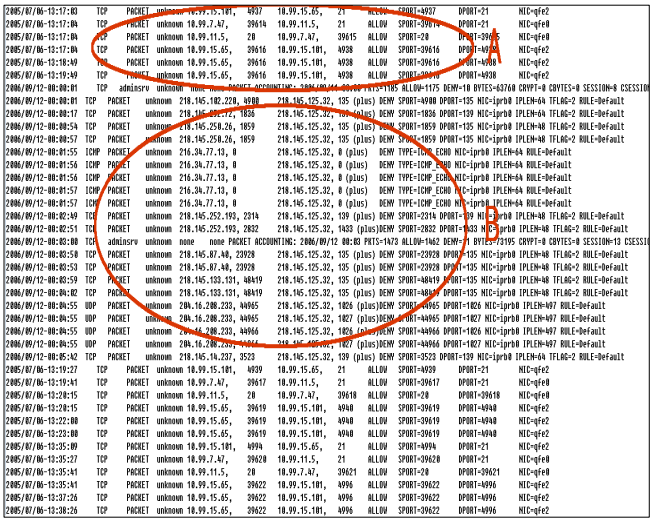
3.1 연구 배경

인터넷 보급의 확산으로 매년 침해사고의 피해가 늘어나는 추세이다. 방화벽과 같은 보안장비가 설치가 되어 있어도 침해사고의 유형이 다양해 관리자가 침해사고 예방을 하기 위해서 기존에 알려진 툴이나 습관에 의존하여 대처를 하게 된다. 이렇게 방화벽 상에서 발생되는

다양한 침해사고를 예방하기 위해 방화벽 로그를 기계학습기법을 통해 보다 빠르고 안정적으로 침입탐지에 사용할 수 있고, 종합적인 사용자의 정보 및 유형(style)을 유추해 냄으로서 침해사고 대책을 세울 수 있도록 제안하고자 한다.

3.2 방화벽 로그의 구성

방화벽의 종류에 따라 로그 기록은 조금씩 차이가 있지만, 타임스탬프(이벤트, 행위, 통신이 발생한 날짜와 시간), 출발지 주소(트래픽의 출발지 IP주소), 출발지 도메인 이름(트래픽 출발지의 도메인 이름), 목적지 주소(트래픽의 목적지 IP주소), 프로토콜(사용된 IP프로토콜 또는 서비스 이름), 메세지 종류 또는 분류(전송된 메시지의 종류), 포트 주소(메시지가 전송된 TCP또는 UDP 포트), 소켓 주소(메시지가 전송된 소켓 주소) 등의 정보가 로그에 저장되게 된다. 이러한 실시간으로 저장되는 로그에는 정상 접속의 로그와 오류 접속의 로그가 남게 된다. 이런 로그를 가지고 기계학습을 이용한 방화벽 로그분석을 수행 한다.

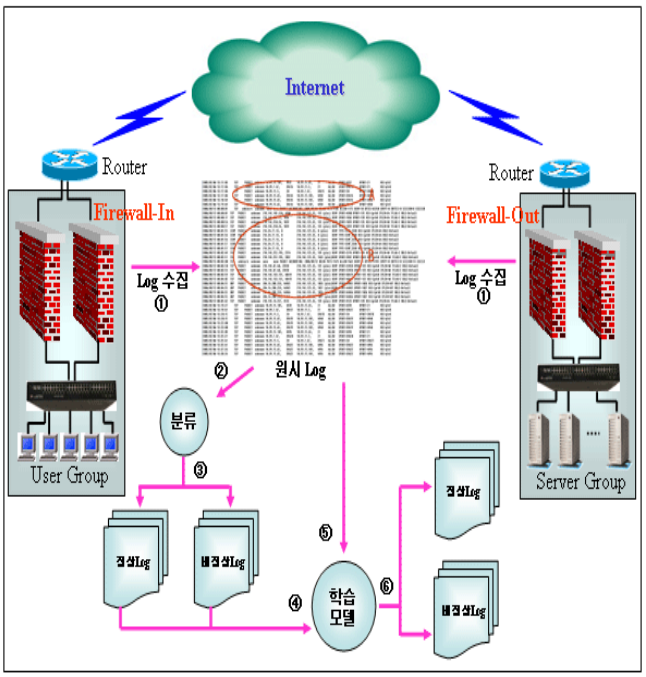


(그림1) 방화벽 원시 로그 파일

(그림1)은 방화벽 원시 로그의 모습이며 A는 정상적인 로그를 보여주고 있는 것이며, B는 오류 로그를 보여주고 있는 것이다.

3.3 기계학습을 이용한 방화벽 로그분석 과정

본 논문에서 제안하는 방화벽 로그 파일 분석 시스템은 방화벽을 통과한 모든 원시로그파일에 관해 정상 로그와 오류 로그로 분류한 후, 기계학습기법을 통해 학습 한 후 학습되지 않은 원시로그를 가지고 정상로그와 오류로그 분석 과정을 보여주고 있다.



(그림2) 방화벽 로그 분석의 구성도

(그림2)는 방화벽 로그 분석의 로그수집부터 분류, 그리고 기계학습에 이르기까지의 전 과정을 보여주고 있으며, 다음과 같은 순서에 의해 수행된다.

① 방화벽 로그 파일의 수집 : 사용자 그룹(Usesr Group)과 서버그룹(Server Group)으로 분리 되어 있는 각각의 방화벽 별로 원시 로그를 추출 한다.
② 학습데이터 분류 : 각 그룹별로 분리된 로그들을 학습데이터에 맞게끔 정상 로그와 오류 로그로 분리를 한다. 이 작업은 관리자에 의해 수동 적으로 분류 작업이 이루어 진다.
③ 학습 데이터 : 정상 로그와 오류 로그로 분류된 학습데이터를 만들고 이를 기계학습의 학습데이터로 사용 한다.
④ 학습 모델 : 기계학습기법의 모델 중 베이지안(Bayesian), 단일의사결정트리, 복수의사결정트리, 신경망(MLP)에 의해 학습을 수행 한다.
⑤ 학습 : 정상 로그와 오류 로그로 분류된 데이터를 가지고 학습을 한 후 새로운 원시 로그를 베이지안(Bayesian), 단일의사결정트리, 복수의사결정트리, 신경망(MLP)에 의해 학습을 수행 한다.
⑥ 학습 결과 : 새로운 학습데이터인 원시로그 파일로 학습된 결과를 정상 로그와 오류 로그로 다시 데이터를 분리 및 저장 한다.

4. 실험 및 분석

본 논문에서는 자동분류를 위해 베이지안(Bayesian), 단일의사결정나무, 복수의사결정나무, 신경망(MLP)기법을 사용한다.

본 논문에서 사용되는 로그는 법무부에서 운영하는 홈페이지(www.moj.go.kr)에서 사용되고 있는 방화벽 2대에서 원시로그를 추출하였다. 이러한 원시로그는 각각의 방화벽 마다 1년치의 로그를 취합 하였고, 방화벽에 남아 있는 로그 중 10개의 분류를 선택하여 표1과 같이 각 분류별로 100개씩의 로그를 선별하여 총 1000개의 로그를 이용하였다.

<표 1> 실험에 사용된 로그 분류

분류번호	분 류	로그수
1	포토스캔 관련	100
2	Service Enumeration 관련	100
3	웜바이러스 관련	100
4	IP Switch IMAIL LDAP 원격 공격 관련	100
5	Dame Ware Probe 관련	100
6	Windows Workstation Service WK SSVC Libc 공격 관련	100
7	MSMQ Heap Overflow 공격 관련	100
8	Windows XP/2000 Return Into Libc 공격 관련	100
9	LSASS.DLL RCP Buffer Overflow 시도 관련	100
10	MS MESSENGER Heap Overflow 시도 관련	100
계		1000

베이지안(Bayesian)학습, 단일 의사결정트리, 복수 의사결정트리는 DTREG 4.5를 이용하였고, 신경망(MLP)기법은 SPSS Neural Connection 2.0 을 이용하였다.

각 분류기에 대한 실험결과는 표2과 같다.

<표 2> 방화벽 로그분석 실험결과 (단위 : %)

분류번호	베 이 지 안 (Bayesian)	단일의사 결정트리	복수의사 결정트리	신경망 (MLP)
1	75	42	84	60
2	64	77	80	69
3	82	72	89	65
4	88	58	90	80
5	81	39	91	69
6	82	62	96	73
7	88	84	99	80
8	70	60	78	64
9	80	71	90	88
10	92	69	90	80
계	80.2	63.4	88.7	72.8

실험결과 복수의사결정트리가 가장 높은 정확도를 보여주었고, 베이지안(Bayesian), 신경망(MLP)기법, 단일 의사결정나무 순의 정확도를 보여주었다.

5. 결론

본 논문에서는 분류되지 않은 방화벽 로그를 기계학습 기법 중 베이지안(Bayesian), 단일의사결정트리, 복수의사결정트리, 신경망(MLP)학습을 이용하여 제안함으로서 보다 빠르게 방화벽 원시로그의 침해여부를 알 수 있었다. 향후 연구과제로 요구되는 부분은 충분한 분류학습기반지식의 확보가 필요하고, 정확한 분류 학습능력 배양을 위한 문서가 요구 되야 할 것이다.

참고문헌

[1] Jeffirey M. Bradshaw "Software Agent" AAAI press/The MIT Press pp151-161

[2] http://www.ncsc.go.kr, 국가사이버안전센터, "방화벽 관리 및 침입기록 분석방법"

[3] T.M. Mitchell. (1997), *Machine Learning.* The McGraw-Hill Companies, Inc

[4] 이 윤성, "인터넷 해킹을 막기 위한 보안 방법 연구", 동아대학교 경영대학원 경영정보학과 석사학위논문, 2000. 12

[5] 송 기욱, "인트라넷에서의 웹 보안 시스템 설계 및 구현 연구", 대전대학교 대학원 정보통신공하고가 석사학위논문, 2001. 2

[6] 오 지우, "로그 데이터 분석에 의한 웹사이트의 비교", 고려대학교 대학원 통계학과 석사학위논문, 2001. 12

[7] 구 성회, "결정 트리를 이용한 침입탐지시스템의 성능분석", 충북대학교 대학원 컴퓨터공학과 석사학위논문, 2002

[8] 차 병래, 박 경우, 서 재현, "이상 침입 탐지를 위한 베이지안 네트워크 기반의 정사행위 프로파일링", 한국컴퓨터정보학회 논문집, 200..3

[9] 이 상영, "효율적인 보안 관리를 위한 방화벽 로그 수집 및 분석 프로그램 구현 연구", 동국대학교 국제정보대학원 정보보호학과 석사학위 논문 2004. 6

[10] 양 대일, 김 경곤, "정보보안 개론과 실습", 한빛미디어, 2005. 5