제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

IBL 을 사용한 네트워크 기반 침입탐지 시스템과 평가 모델의 연구

김도진*, 원일용*, 송두헌**, 이창훈*
*건국대학교 컴퓨터공학과,
**용인송담대학 컴퓨터소프트웨어학과
e-mail : lionguy, clcc, chlee@konkuk.ac.kr
dsong@ysc.ac.kr

A Study on Evaluation Model and Network Based IDS using IBL

Do-Jin Kim*, Il-Yong Won*, Doo-Heon Song**, Chang-Hun Lee*
*Dept. of Computer Science, Kon-Kuk University
**Dept of Computer Software, Yong-In Songdam College

요 약

비정상 행위를 탐지하는 네트워크 기반 침입탐지 시스템은 다른 네트워크 환경에서도 같은 학습정확도와 탐지 성능을 보여야 한다. 그러나 학습을 통한 패턴생성 알고리즘의 특성에 따라 정확도의 불일치가 나타날 수 있으며, 이에 따른 탐지 성능 또한 네트워크 환경에 따라 다르게 보고될 수 있는 가능성을 가진다. 본 논문은 침입탐지를 위한 학습 알고리즘으로 Instance 기반의 알고리즘인 IBL(Instance Based Learning)을 선택하여 학습시간의 단축과 패턴생성에 따른 분류근거의 명확성을 고려하였으며, 학습 환경 즉, 네트워크 환경의 차이에서 나타날 수 있는 정확도의 저하를 고려하여 COBWEB 과 C4.5 로 구성된 평가 요소를 침입탐지 모델에 추가함으로써 네트워크 보안관리자에게 좀더 유연한 비정상 행위 수준 탐지결과를 보고할 수 있게 하였다.

1. 서론

네트워크 기반의 침입탐지 시스템(IDS: Intrusion Detection System)은 담당하고 있는 네트워크 상의 패킷들을 분석한 후 패턴을 생성한다. 생성된 패턴들은 이미 학습된 정상행위 패턴들과 비교되어 매칭되는 정도에 따라 비정상과 정상 행위들로 구분 되어진다.

네트워크의 로우 데이터인 패킷들을 분석하여 비정상의 여부를 판별하는 침입 탐지 시스템에 적용될 수 있는 학습 알고리즘들은 다양하게 존재하며 각각의 알고리즘마다의 특성에 의해 동일한 데이터에도 서로 다르게 반응하며 그 정확도 또한 다르게 나타난다.

침입탐지 시스템은 그 특성상 대용량의 데이터를 다루므로 이를 처리하기 위한 처리속도와 네트워크 사용자의 비정상 행위의 정도를 측정하는 것이므로 판정 근거의 제시가 용이해야 할 것이다.

본 논문은 위에서 서술한 침입 탐지 알고리즘의 적용에 있어 고려되어야 할 사항들을 기반으로 실시간 비정상 행위 IDS 의 설계와 그 구현에 관한 것이다. 제안하고자 하는 시스템은 실시간으로 네트워크상의 패킷들을 원시데이터로 사용하며, 이 원시데이터를 침입탐지를 위해 응용할 IBL(Instance Based Learning) 이 읽어 들일 수 있는 형태로 변환하기 위한 전처리 과정을 거친다. 학습 알고리즘인 IBL 은 패턴을 생성하고 생성된 패턴을 바탕으로 비정상 행위를 구분한다.

평가 모듈은 COBWEB 과 C4.5 로부터 생성된 비정상 행위 정도와 현 침입탐지 알고리즘의 비정상 행위 정도를 비교, 분석하여 네트워크 침입에 대해 유연한 대응이 가능하도록 정보를 제공한다.

2. 동기 및 관련연구

2.1 동기

네트워크 상의 패킷을 대상으로 침입여부를 탐지하기 위한 방법 중 비정상 행위 탐지를 위한 알고리즘으로 Instance 를 기반으로 하는 IBL 을 선택하였다. IBL 은 감독학습 알고리즘으로 Instance 와 Instance 사이에는 유사성이 존재할 것이라 가정하고 각 Instance 의 정보를 나타내는 속성의 평균값을 구하여 이것을 Instance 간 유사도를 측정하는 기준으로 사용한다. 이러한 Classification 알고리즘은 침입 탐지를 다루는 도메인에서 대용량의 데이터를 다루기에 적합하며, 빠른 학습 성능을 나타낸다. 또한 도메인의 특징을 잘 반영하며, 분류근거의 제시가 용이하고, 저용량의 학습지식만으로도 적은 에러율을 나타낸다.

비정상 행위를 탐지하는 침입탐지 시스템은 침입 탐지의 근거를 알고리즘에 의존하며 정확한 분류를 제공하는 알고리즘이라 할지라도 적용 네트워크의 환경과 특정 알고리즘만이 가진 특성에 영향을 받는다. 이러한 이유로 침입 탐지 알고리즘의 비정상 행위도를 평가 할 수 있는 평가 알고리즘을 두어 다른 알고리즘들의 비정상 행위도 결과와 비교, 분석할 수 있는 모듈을 둠으로써 좀 더 유연한 비정상 행위 분류기준을 둘 수 있다.

2.2 IBL(Instance Based Learning)

제안된 침입 탐지 시스템에서 탐지모델의 생성기법은 하나의 사건을 설명할 수 있는 Instance 를 기반으로 하며, Instance 와 Instance 사이의 거리를 나타내는 유사도를 측정하여 패턴을 분류한다. 각 패턴은 PCD(Partial Concept Description)로 구성되며 하나의 PCD 는 패턴을 이루는 Instance 들 중 가장 높은 유사도와 해당 Instance 의 속성값들로 구성되며, 학습과정에서 생성된 PCD 는 하나의 Instance 를 처리할 때 마다 계속 업데이트함으로써 분리 패턴을 생성하게 된다.

IBL 의 학습과정은 [그림 3]과 같이 3 단계로 분리되며 각 단계는 Instance 를 받아들여 일반화하여 학습을 위한 일반화된 Instance 를 생성하는 Processed Instance 를 생성하는 Pre-Process, 유사도 측정과 분류될 카테고리를 예측하기 위한 Prediction 을 생성하는 Performance Component, 다시 Processed Instance 를 받아들여 개념정보인 PCD 를 생성하고 이를 업데이트하는 Learning Component 로 구성된다.

2.3 평가(Evaluation) 알고리즘

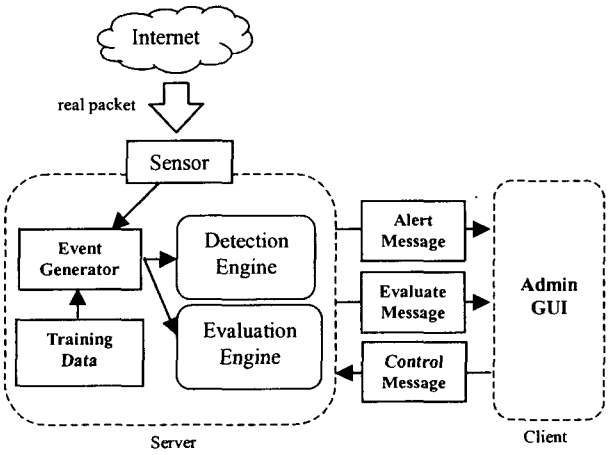
탐지 알고리즘을 구성하기 위해 계층형 개념 군집화(Hierarchical Conceptual Clustering)학습 알고리즘으로 알려져 있는 COBWEB 과 결정 트리 생성기법인 ID3 의 단점을 보완하여 개발된 C4.5 를 적용하였다.

COBWEB 은 인간이 사물을 분류하는 과정인 점진적 개념 형성(Incremental Concept Formation)을 모델로 하여 개발되었다. 이것은 사물을 하나씩 관찰하여 개념을 형성하면서 하향 분류하는 방법이다[5]. COBWEB 은 레코드로 구성된 데이터들을 입력으로 받아, 트리의 형태로 클러스터링을 한다. 트리의 각 노드는 하나의 개념이 되고, 각 노드에는 속성값이 요약되어진 개념정보를 저장하고 있다. 개념 정보는 속성값의 도메인별 확률값이나 평균과 표준편차이다. 속성이 명목형(Nominal) 도메인인 경우에는 확률값이고, 연속형인 경우에는 평균과 표준편차가 된다. 개념정보는 새로운 레코드의 부류를 결정하는데 사용되는 정보가 된다.

C4.5 는 ID3 의 확장 알고리즘이다. ID3 가 가지고 있던 문제점들의 해결 방법으로 Local minimum 을 해결하기 위해 Working Set 과 Training Set 을 분리했으며, Pruning 기법을 이용하여 Leaf 의 Class 가 확률로 표시되고, 속성값이 불완전한 경우에도 판단이 가능하다. 수치데이터의 경우 Thresh hold 에 가까운 데이터의 문제점을 보완하였다. 결정 트리 생성과정은 속성값에 따른 경우의 수를 계산하여 트리를 생성한 후 각 Case 에 따른 무질서도를 계산하여 무질서도가 낮을수록 우수한 카테고리로 분류하게 된다. 생성된 트리는 복잡도를 줄이기 위해 Pruning 기법을 사용하며, Noise 와 정보의 손실 가능성을 고려하여 Leaf 가 분류될 Class 를 확률로 표현한다.

3. 침입 탐지 시스템 구조

본 논문에서 제안하고자 하는 침입 탐지 시스템은 아래 [그림 1]과 같은 구조로 구성된다.

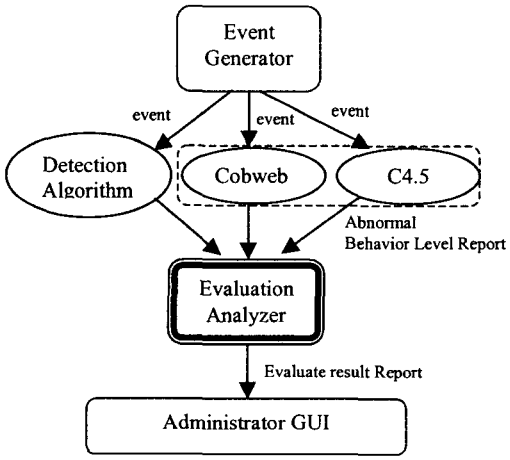


[그림 1] 침입 탐지 시스템의 전체 구조

먼저 시스템은 클라이언트와 서버로 나눌 수 있으며, 서버는 학습 모드를 통해 원시 데이터인 네트워크 패킷을 추출하여 가공한 Off-line Dataset 을 전달한다. 처리과정을 통해 Instance 를 생성하고, 생성된 Instance 는 IBL 알고리즘에 의한 학습으로 탐지 모델을 구성한다.

침입 탐지 모드에서는 네트워크로부터 들어오는 패킷들을 Event Generator 에 의해 Instance 화 하고 이것을 탐지 엔진에 보내게 된다. 탐지 엔진은 학습과정에서 생성한 침입 탐지 모델을 근거로 Instance

들을 분류하여 비정상 행위를 구별하며 비정상 행위에 따른 Alert Message 를 소켓통신을 이용하여 클라이언트인 Administrator GUI 에 보내게 된다. 이렇게 생성된 침입 탐지 모델의 비정상 행위도의 평가를 위해 평가 엔진은 침입 탐지 엔진과 같은 전처리 과정을 거쳐 각 평가 알고리즘들이 인식할 수 있는 데이터들로 변환하게 되고 평가 알고리즘들의 결과와 침입 탐지 알고리즘의 비정상 행위도를 비교, 분석하여 관리자에게 보고하게 된다. 평가 엔진의 구성과 처리 과정은 [그림 2]와 같다.



[그림 2] 평가 엔진의 구성

평가 엔진이 포함하고 있는 두 알고리즘은 침입 탐지 알고리즘과 같이 Event Generator 로부터 Instance 로 변환된 Event 들을 받아들이고, 학습에 의한 정확도를 계산한다. 평가 엔진은 탐지 알고리즘과 Cobweb, C4.5 로부터 각각의 비정상 행위도를 넘겨받아 비교, 분석한 후 Evaluation Analyzer 에 의해 관리자에게 그 결과를 보고한다.

4. 설계 및 구현

4.1 Event 생성

비정상 행위 탐지 시스템은 수집된 방대한 양의 감사 기록 정보들로부터 의미있는 정보로의 전환 및 축약시키는 단계가 필요하게 되는데 이와 같은 전처리 기능을 실행하는 것이 Event Generator 이다. 센서는 Event Generator 에게 실시간으로 수집한 감사 기록 정보인 네트워크 패킷들을 보내게 되는데 이때 수집되는 데이터들로부터 비정상 행위를 구분하기 위한 판정 요소를 추출한다. 아래 [표 1]은 감사 기록정보로부터 추출하기 위한 판정 요소들이다.

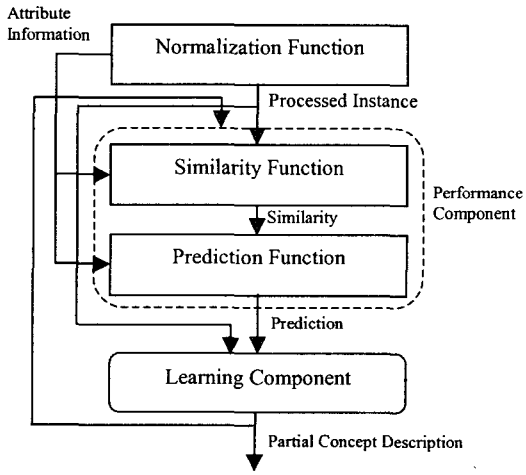
종 류	속 성
공 통	- 탐지 네트워크상의 IP 패킷수 - TCP, UDP, ICMP 패킷수 및 비율
TCP/IP	- TCP 패킷 비율 : Inbound, Outbound - Connection : SYN, SYN/ACK, ACK 비율 - SYN 을 보낸 출발지 IP 의 수 - FIN, RESET 비율 - TCP 헤더의 플래그 비트 값 - TCP payload 의 길이 총합
UDP,ICMP/IP	- UDP 패킷 비율 : Inbound, Outbound - UDP payload 의 길이 총합 - ICMP 패킷 비율 : Inbound, Outbound

[표 1] 이벤트 데이터를 위한 구성요소

본 논문에서는 네트워크상의 의미적인 트랜젝션의 단위를 정의하는 기준을 하나의 패킷으로 정하여 이벤트를 생성한다. 이를 통해 어떤 시점에서 발생된 네트워크 행위를 보다 정확하게 모델링할 수 있다. 위에서 기술한 내용과 같이 판정 요소로써 속성들을 정의하고 그것에 해당하는 속성값을 할당하면 하나의 패킷에 따른 Event 를 생성하게 된다.

4.2 침입 탐지 모델

침입 탐지 모델의 알고리즘은 IBL 을 사용하였다. 학습을 위한 학습모드와 비정상행위를 탐지하기 위한 탐지 모드로 나뉘어져 동작하며, 각각의 Instance 들의 정보를 의미하는 속성 사이의 유사도에 기반하여 그 정도에 따라 분류하게 된다. IBL 의 패턴형성 과정을 살펴보면 아래 [그림 3]과 같다.



[그림 3] IBL 의 패턴생성 과정

모든 Instance 의 속성들은 numeric-value 또는 Symbolic-value 로 채워진 속성값들로 구성된다. 이러한 Instance 의 속성값들 중 가장 높은 값과 가장 낮은 값을 탐색한 후 선택된 속성들을 제외한 모든 Instance 들은 linear normalizing 과정을 거치게 된다.

$$Normalize\ \_attribute\ (x_z, a) = \frac{x_a - a_{\min}}{a_{\max} - a_{\min}}$$

위의 과정으로 일반화된 속성값들은 Performance Component 에 의해 Instance 사이의 관계를 설명하기 위한 유사도와 입력된 Instance 가 특정 카테고리에 속할 수 있는 예측치를 결정한다. 아래의 두 함수는 Similarity function 에 속하며 속성간의 거리를 측정하고 이것을 이용하여 속성사이의 유사도를 도출한다.

$$Similarity\ (x, y) = \frac{1}{\sqrt{\sum_{i \in p} Attribute\ \_defference\ (x_i, y_i)}}$$

$$Attribute\_difference(x_i, y_i) = (x_i - y_i)^2 \quad i\ is\ numeric\text{-}valued$$
$$= x_i \neq y_i \quad otherwise$$

Similarity Function 에 의해서 계산된 유사도를 바탕으로 Instance 들을 묶고, 이렇게 묶인 k 개의 가장 유사한 Instance 들 중 가장 유사도가 높은 Instance 의 속성값들을 Learning Component 에게 넘겨 주는데 이때 이것을 Prediction 이라 한다. 이렇게 생성된 Prediction 을 기반으로 분류된 학습데이터에 대한 정보를 업데이트한다.

학습 모드에서 생성된 패턴들은 학습 모드와 동일한 방법으로 패턴들을 찾아 분류하게 된다. 분류된 패턴들 중 그 정도가 임계치 이상인 것들만을 선택하여 탐지 결과를 관리자에게 보고한다.

4.3 평가 모델

평가 모델은 [그림 2]에서와 같이 COBWEB 과 C4.5 그리고 Evaluation Analyzer 로 구성되어 있다. 두 평가 알고리즘 모두 IBL 과 동일한 Event Generator 를 사용하며 평가 엔진의 동작은 관리자가 탐지 알고리즘의 정확도의 검증작업 시 Server 측에 소켓통신을 통한 메시지를 보냄으로써 동작하게 된다. 관리자로부터 메시지를 받은 평가 알고리즘들은 탐지 알고리즘과 동일한 Event 를 부여 받아 학습과정을 거치고 각 알고리즘들의 패턴생성에 의한 비정상 행위 탐지율에 기반하여 평가분석기는 탐지 엔진의 탐지율과 비교· 분석 결과를 관리자에게 보고한다.

비교, 분석 결과에 따른 침입 탐지 알고리즘의 침입탐지정확도가 낮게 나타내면 평가 알고리즘의 학습으로 생성된 패턴을 이용하여 비정상 행위를 탐지한 뒤 보고된 로그데이터를 바탕으로 적절한 보안 정책 수립이 가능하게 된다.

5. 구현환경 및 실험 방법

본 논문에서 제안하는 시스템은 서버와 클라이언트로 구성되어 있다. 서버는 Linux 환경에서 개발되었으며 탐지 대상이 되는 네트워크의 직접 배치되어 그 기능을 수행할 수 있다. 클라이언트는 서버와 같은 네트워크 또는 다른 네트워크에 배치되어 소켓통신을 함으로써 침입탐지 결과 또는 평가 결과를 보고 받을 수 있다. 실험을 위해서 각 알고리즘들의 환경에 따른 침입 탐지 패턴에 대한 차이를 보이기 위해 표준 환경으로 DARPA 산하 MIT Lincoln Lab 에서 제공하는 Tcpdump 데이터를 사용하였다. DARPA 데이터는 정상 패킷과 smurf 와 syslog 와 같은 서비스 거부공격으로 이루어진 비정상 패킷들이 포함되어 있다. 비교대상의 네트워크는 하나의 패쇄 네트워크를 구성하여 DARPA 데이터와 동일한 방법으로 생성된 Tcpdump 데이터를 사용하였다.

6. 결론 및 향후과제

본 논문에서 제안하는 시스템은 기존의 시스템과는 달리 탐지 알고리즘을 평가하고 평가된 결과를 바탕으로 유연한 보안정책을 수립할 수 있으며, IBL 알고리즘을 적용함으로써 명확한 분류근거의 제시와, 패턴을 생성하기 위한 시간과 자원의 낭비가 감소된다는 점이다. 그러나 평가 알고리즘들과 탐지 알고리즘의 상호보완을 위한 기능은 수행상 많은 자원이 필요하게 되며, 이것은 실시간 침입 탐지 시스템의 치명적 약점이 될 수 있다. 또한 네트워크 공격의 다양성에 대처하기 위해서는 더 광범위한 비정상 행위를 탐지하기 위해 이벤트를 구성하기 위한 판정요소의 선택에 따른 고려가 필요할 것이다.

참고문헌

[1] David W. Aha, "A Study of Instance-Based Algorithms for Supervised Learning Tasks", Department of Information and Computer Science University of California, Technical Report , 1990

[2] Cost & Salzberg, "A weighted Nearest Neighbor Algorithm for Learning with Symbolic attribute feature", Journal of Machine Learning, 1993

[3] Kathleen McKusick, Kevin Thompson, "COBWEB/3: A Portable Implementation", Technical Report FIA-90-6-18-2, AI Research Branch, NASA Ames Research Center, 1990

[4] 이정현, "네트워크 기반 비정상 행위에 대한 다계층 침입 탐지 시스템 설계 및 구현", 석사학위논문, 건국대학교 컴퓨터 공학과, 2001

[5] 이효승, "COBWEB 을 사용한 비정상행위도 측정을 지원하는 네트워크 기반 침입탐지 시스템 설계", 석사학위논문, 건국대학교 컴퓨터 공학과, 2002

[6] 김주영, 강창구, 이극, 이소우 "네트워크 패킷 분석을 통한 침입탐지 기법 개발", 1999

[7] Giovanni vigna, Richard A. Kemmerer, "NetSTAT: A Network-based Intrusion Detection Approach", 1999

[8] J.Frank, "Artificial Intelligence and Intrusion Detection", NCSC, 1994

[9] Murthy and Salzberg, "A System for Induction of Oblique Decision Tree", JAIR 94, 1994