IDS의 False Alarm 발생율 감소를 위한 데이터 마이닝 기반의 분류모델

전원용[0] 신문선 김은희 류근호
충북대학교 데이터베이스 연구실
{ chonwy2000[0], msshin, ehkim, khryu }@dblab.chungbuk.ac.kr

Data Mining based Classification Model for False Alarm rate reducing of IDS

Won Yong Chon[0], Moon Sun Shin, Eun Hee Kim, Keun Ho Ryu
Database Laboratory, Chungbuk National University

요 약

IDS에서 발생되는 경보의 수는 최근 인터넷 애플리케이션의 발달로 인하여 급격히 증가하고 있으며, 그로인해 오 경보의 수도 함께 증가하고 있다. 발생된 경보들은 침입탐지 시스템의 성능저하와 alert flooding 의 원인이 된다. 따라서 이 논문에서는 다량의 경보 중에서 오 경보(False Alarm)의 발생을 감소시킬 수 있는 오 경보 분류 모델을 제안한다. 제안된 오 경보 분류 모델은 데이터 마이닝 기법들 중에서 분류 기법을 기반으로 구현되었다. 실험 을 통해서 IDS에서 발생하는 경보 중에서 정상데이터이나 공격으로 잘못 판단하여 발생하는 False Positive의 발생율이 현저히 감소됨을 확인할 수 있었다. 제안된 오경보 분류 모델은 경보메시지 축약의 효과가 있으며 침입탐지 시스템의 탐지율을 높이는데 활용될 수 있다.

1. 서 론

최근 인터넷의 발전 속도와 비례하여 네트워크 공격기법도 다양해지고 있으며, 그 수도 증가하고 있다. 전통적인 공격은 이미 잘 알려져 있어 방화벽이나 침입탐지 시스템(IDS) 등에 의하여 쉽게 탐지되고 있다. 하지만 지속적인 새로운 공격에 대해서 대응하는 데는 한계가 있다. 그 결과로서 IDS에서는 새로운 공격들에 대한 수많은 경보들을 발생하게 되고 그로 인해서 시스템 부하뿐만 아니라 오히려 다량의 경보들로 인한 Alert Flooding 이 발생할 수 있다. 또한 오 경보(False Alarm) 발생율이 너무 높으면 IDS의 탐지 결과를 신뢰할 수 없으며, 경보 간의 상관관계 분석이나 고수준의 의미 분석을 할 수 없기 때문에 분석된 결과의 신뢰성이나 효율성 또한 저하된다.

이 논문에서는 IDS에서 발생되는 경보 들 중에서 오 경보의 발생 율을 감소시킬 수 있는 오 경보의 분류 모델을 제안한다. 제안된 오 경보분류 모델은 데이터 마이닝 기법 중에서 분류 기법을 기반으로 오경보들 중에서도 정상행위인데도 IDS에서 공격으로 오인하여 발생되는 오 경보(False Positive)를 분류해내는 기능을 수행한다. 이 논문에서는 분류 속성 선택을 위해 연관규칙을 기반으로 한 접근방안을 제시한다. 구현된 오 경보 데이터 분류 모델은 오경보율을 최소화하므로 경보데이터의 분석 및 통합을 통해 경보메시지의 축약 및 침입탐지시스템의 탐지율을 높이는데 활용될 수 있다.

2. 관련연구

IDS에서 발생되는 경보들 중에는 잘못 판단하여 발생된 오 경보를 많이 포함하고 있다. 최근에 오 경보 발생을 최소화하여 IDS 의 성능향상을 위한 연구들이 많이 진행되고 있다. 오 경보 최소화를 위한 연구들로서 시스템 log 데이터 상관관계 분석과 경보 상관관계[1][2]분석 등이 수행되었다. 이들 연구의 문제점은 log 데이터는 시스템에 의존적인 데이터이기 때문에 실질적인 경보를 줄이는 데는 한계가 있다. 최근에는 마이닝 기법을 이용하여 경보 최소화를 위한 연구[3][4]들이 진행되었다. 특히 마이닝 기법 중에서도 연관 규칙을 이용하여 IDS 경보 스트림의 특징을 파악하여 경보를 최소화 하였다. 그러나 연관규칙과 빈발에피소드를 이용하게 되면 중복된 경보 패턴 생성과 빈번하지 않은 경보발생의 문제를 가지고 있다. 이러한 문제를 해결하기 위해서 클러스터링 기법을 사용한 연구도 진행되었다[5]. 이 논문에서는 IDS에서 발생된 경보를 분류하여 오 경보를 식별하여 오경보의 발생을 줄이고자 한다. 다음 장에서는 이 논문에서 제안한 오경보 분류 모델에 대해서 자세히 기술한다.

이 논문의 구성은 다음과 같다. 2장에서는 경보데이터에 대한 관련연구를 기술하고, 3장에서는 제안된 오 경보 분류 모델에 대해서 기술한다. 4장에서는 실험평가를 통해 오 경보 발생율이 현저히 감소되었음을 보여준다. 마지막으로 5장에서 결론으로 끝으로 맺는다.

3. 오 경보 발생 감소를 위한 분류 모델

오 경보(False Alarm)는 실제 정상 행위이지만 IDS에서 정상 행위를 침입으로 잘못 탐지(False Positive)하거나, 실제 공격 행위를 정상행위로 탐지(False Negative)하는 것을 말한다. 즉, 공격의 판단은 표1과 같이 나타낼 수 있다. 이러한 오 경보의 발생은 네트워크 전반에 걸친 보안 서비스의 질을 하락시키는 주요 원인이 된다.

이 연구는 한국전자통신연구원의 정보보호연구원의 연구비 지원으로 수행되었음

표 1. 공격의 판단

Standard metrics		Predicted Connection Label	
		Normal	Intrusions
Actual Connection Label	Normal	True Negative(TN)	[illegible]
	Intrusions	False Negative(FN)	True Positive(TP)

이 논문에서는 오 경보들 중에서 False Positive에 해당하는 오 경보를 감소시키는데 초점을 맞추어 분류 모델을 설계하였다. 분류 모델은 데이터 마이닝 기법 중에서 결정트리기반의 분류알고리즘을 적용하였다[6][7].

아래 그림1은 오 경보 분류 모델에 대한 전체 아키텍처를 나타낸 것이다.

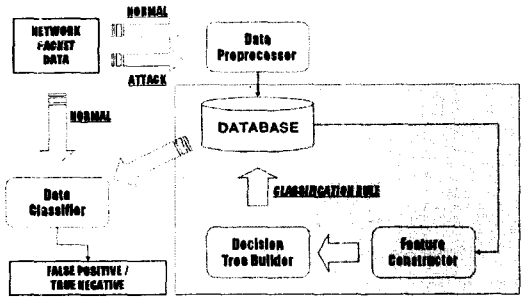

그림 1. 오 경보 분류 모델 아키텍처

오 경보 분류 모델은 먼저 수집된 네트워크 패킷데이터를 가지고 데이터 전처리 과정을 거친 후 데이터를 미리 정의된 클래스 별로 분류한다. 그리고 , 탐지된 데이터베이스 정보로부터 새로운 레코드를 자동적으로 분류할 수 있는 분류 규칙을 생성한다. 그래서 새로운 네트워크 패킷이 들어오면 오 경보 분류 모델에서 분류 규칙에 의하여 공격인지 정상인지를 판별하게 된다. 그 결과로서 침입 탐지 시스템에서 발생될 경보 중 오 경보 발생 율이 감소된다.

오 경보 분류 모델의 전체 처리 과정은 다음의 3단계로 이루어진다.

단계 1 :오 경보 전처리
단계 2 :훈련 데이터를 이용한 분류규칙 생성
단계 3 :실험 데이터를 이용한 분류 모델의 정확도 평가

단계 1에서는 오 경보 분류 모델을 구축하기 위한 오 경보 전처리 단계이다. 이 단계에서는 오 경보 데이터 값의 변환, 잘못된 값을 가진 데이터 수정 및 오 경보 분류 모델 구축을 위한 적합한 속성 선택 등의 작업을 수행하게 된다. 속성을 선택하는 방법에는 여러 가지가 있을 수 있으나 이 논문에서는 데이터 마이닝 기법 중 연관규칙을 이용하여 생성된 결과로서 오 경보 분류 모델의 속성으로서 사용한다.

단계 2는 오 경보 분류 모델 구축 및 분류 규칙을 생성하는 단계이다. 먼저 오 경보 분류 모델 구축을 위해서 단계1에서 선택된 속성들을 가지고 오 경보 분류 모델을 생성한다. 오 분류 모델을 구축하는 단계는 다음과 같다. 1) 각 속성들의 정보값을 구하고 식(2)불순도(순수도)를 측정한다. 불순도 함수로는 엔트로피 지수를 이용하였다.

$$Information = -\log_2 p \quad (p = \text{속성의 개수}) \quad \text{식(1)}$$

$$Entropy(S) \equiv -p_{FP}\log_2 p_{FP} - p_{TP}\log_2 p_{TP} \quad \text{식(2)}$$

오 경보 분류 모델에서 각 노드들이 가지는 내부 항목, 즉 속성들이 가지고 있는 이산적인 값들에 대해서도 불순도를 식(1), 식(2)와 같은 방법으로 측정한다. 측정된 각각의 엔트로피 값을 이용해 최종적으로 정보이득율을 계산하게 되는데 식(3)과 같은 방법을 이용하여 계산한다.

$$Gain(S,A) = Entropy - \Sigma \frac{|S_v|}{|S|} Entropy(S_v) \quad \text{식(3)}$$

(S: 마디가 가지는 클래스 라벨의 갯수, Sv :가지가 갖고 있는 클래스 라벨의 개수)

오 경보 데이터를 분류하기 위한 일련의 과정을 그림 2에서 묘사하였다.

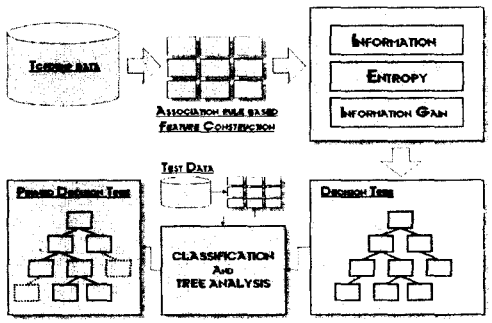

그림 2. 오 경보 분류 과정

그림 3는 연관규칙을 기반으로 하여 생성된 오 경보 분류 모델을 트리 기반으로 묘사한 것이다. 정보이득율이 가장 높은 ACK 를 루트로해서 각 속성을 비교하여 공격 여부를 판단한다.

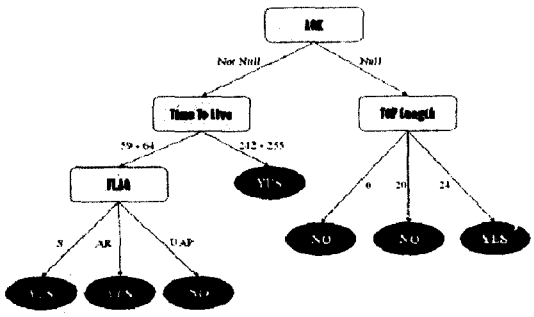

그림 3. 예제: 연관 규칙 기반의 오 경보 분류 모델

그림 4 는 구현된 프로토 타입의 인터페이스를 나타내고 있다. 그림에서와 같이 모델생성단계, 분류단계, 결과보기 세 부분으로 구성 된다.

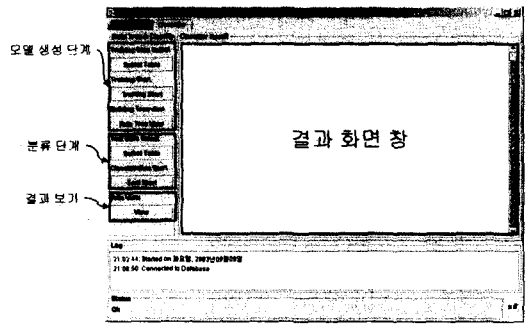

그림 4. 경보 분류 모델 프로토타입

4. 실험평가

마지막으로 단계3에서는 결정트리 모델을 통과한 패킷 데이터가 침입탐지 시스템의 False Positive 생성에 어느 정도의 유용함을 가지는지를 평가하는 실험이다. 실험 환경은 운영체제는 클라이언트 측은 Windows XP, 서버 측은 Linux 7.1를 사용하였다. DBMS 는 Oracle 8.1.7 을 사용하였고, 오 경보 분류 모델 생성을 위해 Java를 사용하였다. 실험 데이터로서 사용된 데이터는 1998년 DARPA Data로서 총 7주간의 네트워크 패킷으로 구성된 Tcpdump 데이터를 사용하였다. 이 데이터 집합은 약 5,000,000개의 데이터 인스턴스로 구성되어 있으며 네트워크 환경 상에서 가능한 다양한 형태의 침입을 포함하고 있다. 이 데이터 중 1-4 주 데이터를 훈련데이터로 사용하였고, 5-7주 데이터를 평가데이터로 사용하였다. 공격의 범위는 서비스 거부 공격(DoS)으로 한정 하였다. 오 경보 분류 모델의 정확성 평가를 위해서 원래의 IDS (여기서는 Snort1.8.6 사용)와 상관관계 기반, 우리의 연관규칙 기반 그리고 두 방식을 혼합한 방법을 사용하여 실험을 하였다. 그림 5는 결정트리를 통과하기 이전과 이후의 False positive탐지율의 변화이다. 전반적으로 결정트리 기반 분류모델을 통과한 이후의 False positives 발생 율이 낮게 나왔으나 6주차 데이터의 경우 결합모델을 제외한 두 개의 모델은 그렇지 못했다.

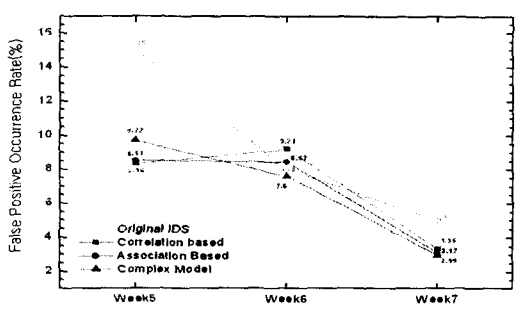

그림 5. 분류모델별 오 경보발생 비율

특징적인 결과를 분석하였을 때 5주차에서는 침입탐지 시스템이 공격으로 오인하는 데이터의 대부분이 근원지 주소와 목적지 주소가 동일한 Land 공격이기 때문에 침입탐지 시스템의 False positive 생성 율이 다른 주차에 비해 높았다. 그 이유는 Land 공격이란 몇몇 시스템에서 TCP/IP 구현상의 문제로 인하여 수신하는 SYN 제어패킷의 출발지주소와 목적지 주소가 해당 패킷을 수신하는 시스템의 IP주소를 가지는 경우 이를 제대로 처리하지 못하고 멈추게 되는 현상이기 때문이다.

5. 결론

네트워크 기반 침입탐지 시스템은 패킷데이터 분석을 통해서 공격 패턴을 탐지한 후, 관리자에게 경보를 전달하는데 그 중에는 많은 오 경보를 포함하고 있다. 오 경보의 수가 많아지면 시스템의 부하나. 오경보로 인한 Alert Flooding 공격이 발생 할 수도 있다.

이 논문에서는 이 문제를 해결하기 위해서 데이터 마이닝 기반의 오 경보 분류 모델을 구현하였다. 특히, 오 경보 중에서도 False Positive를 감소하는 데 초점을 맞추었다. 실험을 통해서 제안된 오 경보 분류 모델에서 서비스 거부 공격에 대한 False Positive 발생 율이 현저히 감소되었음을 확인할 수 있었다.

참고문헌

[1]M. S SHIN, K H RYU."Data Mining Methods for Alert Correlation Analysis" International Journal of Computer &Information Science, Vol. 4 , No. 4 , December 2003

[2]H. Debar and A.Wespi, "Aggregation and Correlation of Intrusion-Detection Alerts", In Recent Advances in Intrusion Detection, number 2212 in Lecture Notes in Computer Science, p 85-103, 2001

[3]Klaus Julisch, Marc Dacier, "Mining intrusion detection alarms for actionable knowledge",18th ACM SIGKDD international conference on Knowledge discovery and data mining , Canada , p 366 - 375, 2002

[4]W.Lee, S.J.Stolfo, "A Data Mining Framework for Building Intrusion Detection Models"Columbia University, Computer Science Department, 2001

[5]신문선, 문호성, 류근호, 장종수, "클러스터링기법을 이용한 침입탐지시스템의 경보상관관계분석", 정보처리학회 논문지C 제 10-C권 p.665-674, 2003,10

[6]C. Kruegel, T. Toth, "Using decision trees to improve signature-based intrusion detection", RAID, 2003

[7]M. S. Shin, K. H. Ryu, "Applying Data Mining Techniques to Analyze Alert Data", APWeb'03, 2003