결정트리를 이용한 IDS의 False Positive 감소기법

정경자*
*충청대학 디지털마케팅과
e-mail: kjeong@ok.ac.kr

False Positive Reduction for IDS using Decision Tree

KyeongJa Jeong*
*Dep't of Digital Marketing, ChungCheong University

요 약

침입탐지시스템은 공격이라고 판단되면 경보를 발생하여 보안 관리자에게 알려주거나 자체적으로 대응을 하게 된다. 그러나 이러한 경보들 중에 오경보가 많이 포함되어 있어 침입탐지시스템의 성능을 저하시킬 뿐 아니라 대량의 경보자체가 보안메커니즘에 방해가 되고 있다. 특히 오경보중 False Positive가 전체 오경보의 대부분을 차지하고 있다. 즉, False Positive는 정상 행위를 침입행위로 오인하여 판단하는 것을 의미한다. 경보들 중 이러한 오경보들은 네트워크 전반에 걸친 보안 서비스의 질을 하락시키는 원인이 된다. 따라서 침입탐지시스템의 성능향상을 위해서는 이러한 오경보 문제가 반드시 해결되어야 한다. 본 논문에서는 침입탐지시스템의 오경보를 감소시키는 결정트리 기반 오경보 분류모델을 제안하였다. 결정트리 기반 오경보 분류 모델은 침입탐지시스템의 오경보율을 감소시키고 침입탐지율을 향상시키는 역할을 수행한다는 것을 확인할 수 있었다.

1. 서론

침입탐지시스템은 공격이라고 판단되면 경보를 발생하여 보안 관리자에게 알려주거나 자체적으로 대응을 하게 된다. 그러나 이러한 경보들 중에 오경보가 많이 포함되어 있어 침입탐지시스템의 성능을 저하시킬 뿐 아니라 대량의 경보자체가 보안메커니즘에 방해가 되고 있다.공격의 판단은 [표 1]과 같이 나타낼 수 있다.

[표 1] 공격을 평가하는 표준 메트릭

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

실제 침입과 침입이 아닌 정상행위에 대해 4가지로 판단 할 수가 있다. 1) 정상행위를 정상행위로 판단하는 경우(TN), 2) 침입행위를 침입으로 정확히 탐지하는 경우(TP), 3) 정상행위를 침입으로 오인하는 경우(FP), 4) 침입을 정상행위로 오인하는 경우(FN)이고, 오경보라는 것은 3)과 4)의 경우를 말하고 있으며 이중 3)False Positive가 전체 오경보의 대부분을 차지하고 있다. 즉, False Positive는 정상 행위를 침입행위로 오인하여 판단하는 것을 의미한다. 경보들 중 이러한 오경보들은 네트워크 전반에 걸친 보안 서비스의 질을 하락시키는 원인이 된다. 따라서 침입탐지시스템의 성능향상을 위해서는 이러한 오경보 문제가 반드시 해결되어야 한다. 따라서 본 논문에서는 IDS 의 False Positive 감소를 위해 결정트리 기법을 적용하여 오경보율을 감소시키는 오경보 분류모델을 제안한다. 2장에서는 연구배경과 선행연구에 대하여 알아보고 3장에서는 오경보 분류를 위한 속성선택과 분류모델 구축, 4장에서는 실제 훈련데이터와 실험데이터를 토대로 IDS 에 적용한 실험 결과를 기술하며 5장에서 결론을 맺는다.

2. 연구 배경

침입탐지시스템에서는 침입 혹은 공격에 대하여 경보데이터를 발생시킨다. 따라서 보안 관리자는 침입탐지시스템의 경보를 항상 모니터링 하여야 한다. 그러나 대량의 경보데이터 발생과 오경보의 발생 등은 침입탐지시스템의 성능을 저하시키는 결과를 초

래하게 된다. 따라서 경보데이터의 통합 관리와 경보 상관성 분석, 오경보 감소 등을 위해서 경보 데이터를 분석하고, 이를 이용하여 공격의 시퀀스를 추출하고 오경보를 분류하거나 경보데이터 필터링 등을 수행한다.

개연적 경보 상관관계 분석은 경보 데이터의 속성의 유사성을 이용하여 경보 데이터 간의 상관관계를 분석하는 기법이다. [5]에서는 발견 학습을 이용한 접근 방법을 "포트탐지공격(stealthy portscan)"을 탐지하기 위해 적용하였다. 비록 발견 학습을 경보 데이터 상관관계 분석에 이용하였지만, 이 방법 또한 경보 데이터 간의 인과 관계를 완벽하게 분석하지 못하였다.

P.Ning은 경보 데이터의 통합과 상관관계 분석 기법을 제안하였다[2]. 특히, Ning이 제안한 상관관계 분석 방법은 어떤 타입의 경보가 주어진 경보 유형의 다음에 오는지를 기술하기 위한 결과 메커니즘을 이용하였다. 이것은 오용 탐지 기법과 유사하다. 그러나 이 결과 메커니즘은 단지 경보의 유형과 경보에 의한 프로브, 보안 레벨, 결과 정의에 포함된 두 경보 간의 시간 간격만을 사용하며, 가능한 모든 경보 데이터들이 서로 관련되기 위한 충분한 정보를 제공하지 않는다는 단점이 있다. 게다가 공격자가 어떻게 공격의 시퀀스를 조정할 것인지 예측하는 것 또한 쉽지 않다. 오경보중 False Positive가 생기게 되는 원인으로는 패턴 매칭 방식을 이용하기 때문에 침입탐지시스템의 시그네처와 유사한 형태의 패턴을 공격으로 탐지하는 경우이다. False Positive 는 경보데이터 발생 후에 관리자의 분석을 통해 판단할 수밖에 없는 데이터이다.

따라서 False Positives를 분석하기 위해 이미 정상 및 공격으로 검증된 네트워크 패킷 데이터의 속성을 추출하고, 이들 패킷 데이터 중에서 정상으로 판정된 패킷을 침입탐지 시스템에 통과시켜 공격으로 오인하는 데이터를 False Positive로 정의한다. 또한 저장된 네트워크 패킷 데이터는 데이터 마이닝 기법을 통해 분류모델 구축에 사용된다.

3. 오경보 분류 모델 구축

네트워크 패킷데이터는 원시 데이터이기 때문에 관계형 데이터베이스에 저장하기 위해서는 데이터 가공이 필수적이다. 따라서 원시 데이터에서 속성을 추출하여 데이터베이스에 저장하기 위해 전처리 프로세서 모듈을 이용하여 아스키 형태로 변환하였다[4]. 먼저 네트워크 패킷 데이터를 수집하여 전처리 프로세서를 거친 후 연관규칙 기반과 통계적인 분석 기법을 사용하여 유용한 속성들을 선택한다. 구축된 모델은 실험 데이터를 이용하여 분류 규칙을 분석한다.선택된 속성들을 가지고 분류 모델을 구축하기 위해 먼저 루트 속성 결정을 위한 방법으로 정보이득을 계산하고 엔트로피와 정보예측치를 구하여 각 속성에 대한 값을 계산하여 각 노드를 결정하여 모델을 구축한다. 저장된 학습데이터를 이용하여 분류 모델을 구축하기 위한 단계별 수행 내용은 다음과 같다.

○ 속성 선택

의사결정트리의 뿌리마디부터 끝마디까지 사용할 속성들을 결정하는 부분이다. 속성을 선택하는 방법에는 여러 가지가 있을 수 있으나 이 연구에서는 데이터 마이닝 기법중의 하나인 연관규칙의 빈발집합을 이용한 방법과 통계적 분석방법인 상관분석을 이용하여 사용한다. 따라서 이 연관규칙을 이용하여 빈발항목을 찾아냄으로써 각각의 패킷들 간에 강한 연관성을 가진 속성들을 지지도를 기반으로 선택할 수 있는 것이다. 이 논문에서는 마디가 될 속성을 선택하여 속성목록에 저장한다.

상관관계 분석은 둘 또는 그 이상의 변수들 간에 존재하는 상관 관계정도를 분석하는 것을 말한다. 변수들 간의 상호 관계정도를 분석하는 통계적인 기법으로써 이 연구에서는 다중 속성들 간의 분석을 위해 셋 또는 그 이상의 변수간의 관계 정도를 밝히는 방법인 다중 상관관계 분석 방법을 이용하였다. 상관분석을 통하여 각 속성들 간의 상관계수를 계산하여 상관계수가 양적 선형관계에 있는 속성들을 선택하여 결정트리의 마디로 결정한다.

○ 훈련 데이터를 이용한 분류규칙 생성

속성 선택 단계에서 저장된 속성목록의 속성 값들을 마디로 하여 분류모델을 생성하는 과정이다. 먼저 첫 번째로 연속적인 값을 일정한 도메인을 가지는 이산적인 값으로 변환하는 작업을 수행한다. 의사결정트리에서 하위노드로 가지를 생성할 때 연속적인 값을 그대로 사용한다면 불필요한 개수의 가지가 생성되게 된다. 그래서 일정한 범위를 정해 이산적인 값으로 변환하는 것이다. 두 번째로 뿌리 노드 결정 작업을 수행한다. (식 1)에 의해서 각 속성들의 정보

값을 구하고 (식 2)에 의해서 불순도/순수도를 측정한다. 불순도 함수로는 엔트로피 지수를 이용하였다.

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

(식 1)

$$Entropy(S) \equiv -p_{YES}\log_2 p_{YES} - p_{NO}\log_2 p_{NO}$$

(식 2)

각각의 마디들이 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 정보 이득율을 계산하게 되는데 (식 3)을 이용하여 계산한다.

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

(식 3)

(S: 마디가 가지는 클래스라벨의 갯수, S_v: 가지가 갖고 있는 클래스라벨의 개수)

각 속성들에 대해 정보 이득율(Information Gain)을 계산한 후 가장 높은 속성을 뿌리 마디로 결정한다. 세 번째는 중간마디를 결정하는 과정인데 부모노드의 결정과 마찬가지로 각각의 가지에 대해 재귀적인 방법으로 더 이상 분할이 일어나지 않을 때까지 수행한다. [알고리즘 1]은 경정트리 생성 알고리즘을 보여준다.

[알고리즘 1] 결정 트리 생성 알고리즘

```
Algorithm DCTree()
Input   : the training samples (samples), represented by discrete-valued attributes, attribute list
Attribute List : the set of candidate attributes
Method :
  Call DecideNode()
    create a node N;
    if samples are all of the same class, C then return N as a leaf node labeled with the class C;
    if attribute-list is empty then return N as a leaf node labeled with the most common class
       in samples;
    select test-attribute, the attribute among attribute-list with the highest information gain;
    label node N with test-attribute;
    for each known value a_i of test-attribute grow a branch from node N for the condition test-
       attribute = a_i;
    let s_i be the set of samples in samples for which test-attribute = a_i;
    if s_i is empty then attach a leaf labeled with the most common class in samples;
    else attach the node returned by generate_decision_node ;
Output : Decision Tree
```

○ 실험데이터를 이용한 분류 모델의 정확도 평가

훈련 데이터를 이용해 생성한 분류 규칙의 정확도를 평가하는 단계로써 훈련데이터의 일부분을 추출하거나 또는 소량의 실험용 데이터를 이용하여 수행한다. 이를 통해 관리자는 생성된 분류 규칙의 정확도 및 과적용 등을 분석하고 필요한 경우 가지치기를 통해 의사결정트리의 정확도를 높인다.

데이터 분류 알고리즘은 [알고리즘 2]에서 기술하였다. 이 알고리즘은 실험 데이터를 이용한 결정트리의 정확도 검증 및 실제 데이터를 이용한 오경보의 분류에 사용된다.

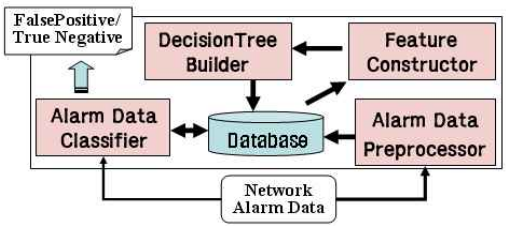
[알고리즘 2] 데이터분류 알고리즘

```
Algorithm False Alert Classifier()
Input   : the test data, represented by discrete-valued attributes, attribute list
Attribute List : the set of candidate attributes
Method :
  Call Classifier()
    1. Load the Decision Tree
    2. Partition into classification rules of IF-Then structure
    3. Counting the number of classification rule
    4. Decision Class Compare given input data to a number of classification rules
    5. 4 repeat until no more exist data
Output : Classification Rule (True Positive/False Positive)
```

4. 오경보 분류 모델 구현 및 실험

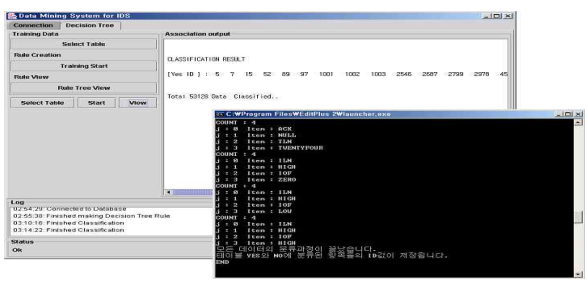
경보데이터 분류 모델을 구현하기 위한 프로그래밍 언어는 JAVA를 이용하였다. 데이터를 저장하는 관계형 데이터베이스로는 Oracle 8i(8.1.7.3)를 이용하였고, 분류시스템의 백그라운드에서 구동되는 침입탐지 시스템은 오픈소스인 스노트버전1.8.6을 사용하였다.

오경보 분류 모델의 전체 구조는 [그림 1]과 같다. 경보데이터 전처리모듈, 속성선택 모듈, 결정트리 생성모듈, 데이터 분류 모듈로 구성되어 있으며 분류규칙의 저장과 전처리된 경보데이터의 저장을 위해서 관계형 데이터베이스를 이용한다.



[그림 1] 오경보 분류 모델 구조

[그림 2]는 구현된 시스템을 보여준다. 분류를 하기 위해 데이터베이스에 저장되어 있는 테이블을 선택하고 분류를 수행하게 되면 규칙집합이 저장되어 있는 규칙 데이터베이스를 불러 각각의 투플들이 이 규칙과 일치하는지를 조건식에 의해 비교한 후 결과값을 출력한다.



[그림 2] 오경보 분류 모델 구축

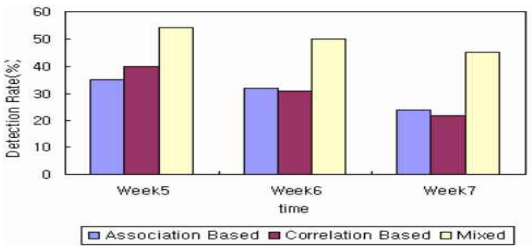
분류 할 테이블을 선택한 후 분류 모델을 구축하기 위해 학습데이터를 이용하여 분류 모델구축을 구축하고 수행이 완료되면 최종 분류 규칙들이 나타나게 된다.

오경보 분류모델은 데이터 마이닝 기법 중 결정 트리를 이용하여 침입탐지 시스템에서 발생하는 수많은 경보데이터 중 잘못된 경보데이터의 일종인 오경보(False Positive) 데이터를 감소시켜 침입탐지 시스템의 성능향상을 가져오는 것을 그 목적으로 한다. 따라서 구현된 경보데이터 분류 모델은 침입탐지 시스템이 네트워크 패킷을 획득하기 이전의 위치에서 동작한다. 경보데이터 분류 모델이 정상행위로 판별한 패킷을 침입탐지 시스템에 통과시킴으로써 탐지율을 측정한다. 또한 앞에서 언급했던 것처럼 훈련 및 테스트 데이터로써 원시 패킷 데이터를 사용하였고, 탐지의 정확도를 높이기 위해 공격의 카테고리는 서비스 거부 공격으로 제한한다. 경보데이터 분류 모델에 대한 평가 항목은 [표 2]에서처럼 정의하였다.

[표 2] 평가 항목

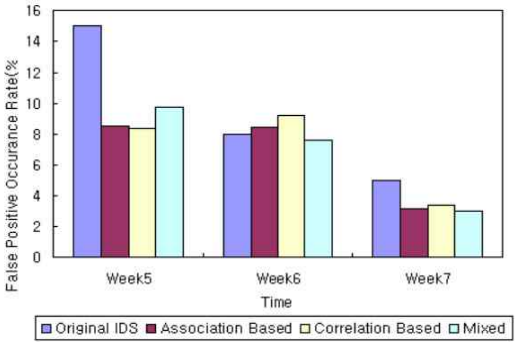
평 가 항 목
○ 속성 선택 방법의 차이에 따른 노드의 변화
○ 속성 선택 방법의 차이에 따른 분류 모델의 정확도
○ False Positive 감소에 따른 침입탐지 시스템의 성능평가

실험 데이터는 1998년 DARPA 데이터 집합[1]중 평가를 위해 공격으로 명시된 데이터 중 서비스 거부 공격들만을 따로 추출하였으며, 정상행위 데이터의 추출은 공격데이터의 전체 크기와 동일한 양의 패킷을 추출하였다. 실험에서는 두 가지의 속성 선택방법을 이용하여 분류 모델의 노드를 결정한 후 두 개의 분류모델을 생성, 5-7주까지의 98년도 DARPA 데이터를 사용하여 생성된 분류 모델의 정확도를 자체 평가한다.



[그림 3] 분류모델별 정상패킷 탐지율

[그림 3]은 상관관계 분석 및 연관규칙의 빈발 항목을 이용하여 얻어진 속성으로 생성된 분류모델과 두 개의 분류 모델을 결합한 후 실험한 결과인 혼합모델인 경우의 실험결과를 보여주고 있다. [그림 4]는 분류모델을 통과하기 이전과 이후의 False Positive 탐지율의 변화이다. 전반적으로 분류모델을 통과한 이후의 False Positives 발생율이 낮게 나왔다.



[그림 4] 분류모델별 False Positive 발생 비율

5. 결론

본 논문에서는 침입탐지시스템의 앞부분 혹은 뒷부분에서 오경보를 감소시키는 경정트리 기반 오경보 분류모델을 제안하였다. 결정트리 기반 오경보 분류모델은 침입탐지시스템의 오경보율을 감소시키고 침입탐지율을 향상시키는 역할을 수행한다는 것을 확인할 수 있었다.

향후 침입탐지시스템의 시그네쳐나 규칙에 추가할 수 있도록 하는 에이전트 개발에 대한 연구가 계속되어야할 것이다.

참고문헌

[1] D. Curry and H. Debar, "Intrusion detection message exchange format data model and extensible markup language document type definition", Internet Draft, draft-ietf-idwg-idmef-xml-03.txt, Feb. 2001.

[2] P. Ning and Y. Cui., "An intrusion alert correlator based on prerequisites of intrusions", Technical Report TR-2002-01, Department of Computer Science, North Carolina State Univ., Jan. 2002.

[3] Moon Sun Shin, EunHee Kim, Keun Ho Ryu, " False Alarm Classification Model for Network-based Intrusion Detection System", IDEAL2004, LNCS, SpringerVerlag,

[4] Moon Sun Shin, HoSung Moon, KeunHo Ryu, JinOh Kim and KiYoung Kim, "Applying Data Mining Techniques to Analyze Alert Data", APWeb2003, LNCS 2642 pp.193-200, SpringerVerlag.

[5] A. Valdes and K. Skinner, "Probabilistic alert correlation", In Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID 2001), pages 5468, 2001.