데이터마이닝을 이용한 감사데이터 학습 방법

정종근 , 김선종 , 김철원 ,
jkjeong@honam.ac.kr

Audit Data Learning Method using datamining

JongGeun Jeong , Sun-Jong Kim , Chul-Won Kim
Dept of Computer Engineering Honam Univ.

요 약

상용화되어 있는 대부분의 IDS는 오용 탐지 방법에 의한 것이다. 그러나 이러한 오용 탐지 방법에 의한 IDS는 침입패턴이 다양화되고 변형되기 때문에 긍정적 결함이 발생한다는 단점을 가지고 있다. 본 논문에서는 감사데이터간의 침입 관계를 가지고 침입을 탐지하기 위해 데이터 마이닝 기법을 적용하여 침입 탐지 시 발생하는 긍정적 결함을 최소화 하였다. 따라서 감사데이터 학습단계에서 변형된 침입 패턴을 예측하기 위해서 데이터 마이닝 알고리즘을 적용한다.

I. 서론

침입판정을 위한 분석 기술은 오용탐지(Misuse Detection)기법과 비정상탐지(Anomaly Detection) 기법으로 구분된다. 오용탐지기법은 일반적으로 침입으로 알려져 있는 오류(Bug)나 행위 또는 비정상적인 행위를 패턴으로 정의하고 수집된 감사사건이 미리 정의된 패턴과 일치하는 경우에 이를 침입으로 판정한다. 일반적으로 오용탐지기법은 패턴매칭(Pattern Matching) 기술을 사용하며 현재 많은 상용제품들이 오용탐지기법을 사용하고 있다. 비정상탐지기법은 정상적인 행위에 대한 프로파일을 생성하고 실제 수집되는 감사 데이터를 프로파일과 비교해 정상행위로부터 벗어나는 비정상행위를 탐지하는 기법이다. 새로운 침입 또는 오용의 탐지에 효율적이라는 장점이 있는 반면, 탐지비용이 높고 악의적인 목적으로 자신의 행위패턴을 서서히 학습시키는 사용자에게는 취약하다[1,4]. 또한 데이터베이스의 정확도에 따라 정상행위를 침입으로 분류하는 긍정적 결함(False Positive) 오류를 범할 수도 있다. 비정상탐지 모델은 데닝의 모델이 기반을 이루고 있는데 현재 많이 적용되고 있는 탐지 모델로는 수량적 분석, 통계적 분석 그리고 신경망 기반 모델 등이 있다. 수량적 분석 모델은 탐지 규칙 또는 속성 값에 수치적인 값을 사용하여 침입 또는 오용을 탐지하는 방식으로써 대표적인 수량적 분석 모델에는 임계값에 기반한 탐지방식이 있으며 현재 많은 IDS가 임계값을 통한 침입탐지방식을 사용하고 있다. 그러나 임계값 기반 비정상탐지 방식은 침입 판정을 위한 정확한 임계값 설정의 어려움으로 인해 긍정적 결함이 증가한다는 문제점이 있다. 현재까지 제시된 침입탐지 시스템들은 몇 가지 문제점들을 공통적으로 가지고 있는데 이 중 가장 두드러진 문제점은 시스템 부하에 관한 것이다. 이를 해결하기 위해 별도의 침입탐지모듈에 의해 네트워크 전체가 분석되도록 하고 있다. 감사 흔적(Audit Trail)을 분석하기 위해서는 시스템 커널이 시스템 상에서 이루어지는 모든 행동들에 대해 감사 정보를 만들어 내야 하는 데, 그 양이 엄청나며 분석 작업에는 시스템의 디스크 용량이나 CPU Time의 엄청난 소모가 필요하다. 따라서, 본 논문에서는 가능한 시스템의 부하를 최소화하기 위해 감사 데이터 표준화 방안을 모색하였고, 막대한 감사 데이터의 양을 효율적으로 축약하는 데이터 마이닝 기법을 적용하였다. 데이터 마이닝 기법은 다량의 패턴 데이터로부터 예측가능한 패턴 데이터를 추출하여 변형된 침입을 탐지하고자 한다.

II. 데이터 마이닝을 이용한 감사데이터 학습

2.1 연관규칙을 이용한 감사데이터 분류

데이터 마이닝의 연관규칙 탐사 알고리즘 중 가장 대표적인 방법이 Apriori 알고리즘이다. Apriori 알고리즘은 여러 논문에서 연구되어 다양한 분야에 응용되고 있다. Apriori 알고리즘은 데이터베이스에서 후보 항목 집합을 구성하고, 구성된 후보 항목 집합에서 빈발 항목 집합을 탐사하는 과정으로 수행된다. Apriori 알고리즘은 후보 항목 생성시 모든 데이터베이스에서의 데이터 항목에 대한 생성이 아닌, 전 단계의 빈발 항목 집합을 대상으로 후보 항목을 생성한다. Apriori 알고리즘은 전 단계에서의 빈발 항목 집합에서 현재 단계의 후보 항목 집합을 구성 한 다음 데이터베이스의 스캔을 통해 후보 항목 집합의 지지도를 계산한다. 그리고, 사용자가 정의한 최소 지지도를 기초로 하여 현재 단계의 빈발 항목 집합을 구성한다. Aprirori 알고리즘의 단계의 진행은 데이터 항목의 증가에 따라 반복적으로 진행된다. k단계에서의 Apriori의 빈발 항목 탐사는 k-1 단계의 빈발 항목 집합으로부터 생성된 k-후보 항목 집합에 대하여 각각의 지지도를 계산한 후 이들 중에서 지지도를 만족하는 항목의 탐사를 통해 이루어진다. Apriori는 더 이상의 후보 항목을 생성할 수 없을 때까지 반복되어 빈발 항목을 탐사하며, 빈발항목 집합의 생성 알고리즘은 [그림 1]과 같다.

```
L1 = {large 1-itemsets}
for (k=2;Lk-1≠Ø;k++) do begin
  Ck = apriori-gen(Lk-1); //새로운 후보항목 집 합
   forall transactions t∈D do begin
  Ct     =     subset(Ck,t);     //후보항목이     빈발항목집합에
          포함
        forall candidates c∈Ct do
          c.count++;
   end
Lk = {c∈Ck | c.count ≥ Smin}//최소지지도를 만족
end
Answer = ∪Lk;
```

그림 1. 빈발 항목 집합 생성 알고리즘

[그림 2]의 알고리즘과 같이 후보 항목 집합의 생성은 전 단계의 빈발 항목 집합의 조인 연산(Join operation)과 전지 과정(Prune process)을 통해 이루어진다. 조인 연산은 두 집합의 곱집합을 구하는 것과 같으며 전지 과정은 조인을 통해 생성된 후보 항목 집합의 부분 집합이 전 단계의 빈발 항목 집합의 원소가 아닌 경우, 그 항목을 삭제하는 과정이다. 그 이유는 전 단계에서 빈발하지 못하는 항목은 다음 단계에서도 빈발하지 못하기 때문이다. 전지 과정은 불필요한 후보 항목의 수를 줄여 데이터베이스를 읽는 횟수를 감소시키기 위하여 추가된 과정이다.

2.2 침입패턴 분류

비정상 탐지를 위한 기계학습 방법의 어려움은 알려져 있지 않은 패턴과 알려진 패턴의 한계를 정하는 것이다. 학습 데이터에 있어서 비정상 패턴에 대한 별다른 예를 가지고 있지 않은 상태에서는 기계 학습 알고리즘은 훈련 데이터에 있는 알려진 패턴에 대한 한계를 구분할 수 없다[5,6]. 일반적으로 비정상과 오용 탐지를 구분하기란 쉬운 일이 아니다. 비정상 탐지는 전형적으로 비통제된 학습 방법을 사용하는 반면에 오용 탐지에서는 통제된 분류 방법을 사용한다[2,3,7].

```
Algorithm Apriori-gen
insert into Ck  // 필요한 항목 추가
select a.item1, a.item2, ···,a.itemk-1, b.itemk-1
from Lk-1a,  Lk-1b
where  a.item1 = b.item1, ···,a.itemk-2:
                = b.itemk-2, a.itemk-1 < b.itemk-1
// 생성된 항목이 전단계의 빈발항목원소가 아닌 경      우 삭제
for all itemset c∈Ck do
  for all (k-1)-subsets s of c do
  if (s∉Lk-1) then
     delete c from Ck;
```

그림 2. 조인연산과 전지과정의 알고리즘

따라서 변형된 패턴의 공격이 발생할 경우 이를 탐지해 내지 못하므로 변형된 새로운 유형의 공격이 발생할 경우, 이 공격 패턴을 즉시 학습시킴으로써 새로운 공격에 대응하고자 한다. 이를 위해 새로운 공격 패턴이 발생할 경우 이미 분류되어 있는 침입 패턴 집합에 계속적으로 추가시킨다. [그림 3]의 알고리즘에서와 같이 H_2는 새로운 침입 패턴과 정상 데이터로부터 학습되어 추가된 분류자이며 알고리즘에서 결정 규칙은 출력을 위해서 평가된다. H_1은 존재하는 침입 탐지 시스템 모델이고 H_2는 최근에 발견된 새로운 침입 패턴을 위해 훈련된 새로운 모델이다. H_1에서는 정상과 비정상 패턴만을 확인하고 새로운 침입을 확인할 수 없기 때문에 대부분의 패턴들은 비정상과 오용으로 분류한다. 그러나 H_2는 새로운 침입과 정상 데이터로 분류한다. 이때 새로운 침입 패턴의 양이 적기 때문에 H_2는 다른 데이터로부터 침입 패턴을 쉽게 분류할 수 있다.

```
Intrusion_learning()
{
if (H1(x)=normal) ∨ (H1(x)=anomaly) then
  //정상패턴과 비정상 패턴 분류
  if H2(x)=normal
    then output ← H1(x)(normal or anomaly)
  //존재하는 침입 패턴 모델
    else output ← new_intrusion
else output ← H1(x)
}
```

그림 3. 침입 탐지 분류 알고리즘

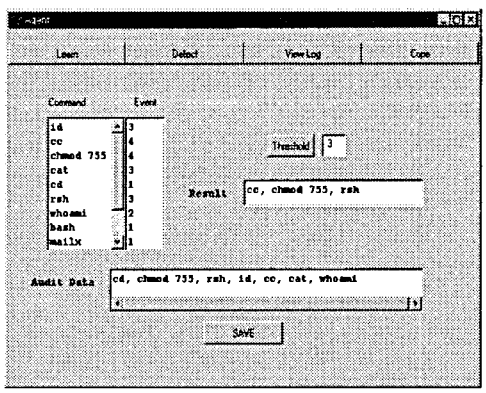

그림 4. 감사데이터 학습 화면

Ⅲ. 구현 및 성능 평가

3.1 침입 탐지 시스템 구현

각 호스트에서 수집된 표준화된 로그 데이터는 이미 침입 탐지 시스템 데이터 베이스에 저장되어 있는 침입 패턴과의 매칭을 통해 침입을 판단한다. 이때 데이터베이스에 저장되어 있는 감사 데이터는 지속적인 학습을 통해 새로운 유형의 침입 패턴을 계속 갱신(update)한다. 또한 미리 정의해 놓은 규칙들로부터 변형된 침입 패턴을 예측·생성한다.

[그림5]는 침입 탐지 모듈에 대한 구성도이다. 에이전트에서 수집한 사용자의 로그 데이터와 침입 패턴(PT)과 비교하여 기대치 이상이거나 일치하는 침입 유형을 찾아서 일치하면 침입 상태를 보고한다. 시나리오에는 없지만 새로운 침입 패턴이라고 판명 될 때는 감사 데

이터 DB에 저장한다.

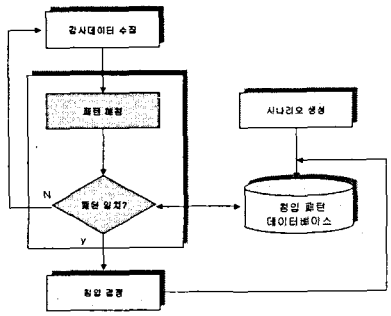

그림 5. 탐지 모듈 구성도

3.2 성능 평가

침입 탐지 시스템의 핵심이 탐지의 정확도와 높은 탐지율이라면 가장 큰 문제점은 탐지 오판율을 최소화시키는 일이다. 침입 탐지 오판의 대부분은 긍정적 결함(false positive)과 부정적 결함(false negative)으로써, 이와같은 결함들을 최소화시키는 것이 오판율을 줄이는 것이다. 본 논문에서는 긍정적 결함을 최소화하는 것에 초점을 두었다. 긍정적 결함의 발생원인은 침입 패턴을 감사 데이터화하는 과정에서 침입 패턴에 대한 감사 데이터 범위를 결정하는 과정에서 발생한다. 이를 해결하기 위해서 본 논문에서는 감사 데이터를 학습하는 과정에서 데이터 마이닝 기법을 적용하여 하나의 침입 패턴에서 발생할 수 있는 여러 가지 변형 형태에 대한 예측 학습이 가능하도록 하여 긍정적 결함의 발생을 최소화하였다. [그림6]은 임계값(threshold)이 증가함에 따라 긍정적 결함이 감소하는 실험 결과를 보여주고 있다.

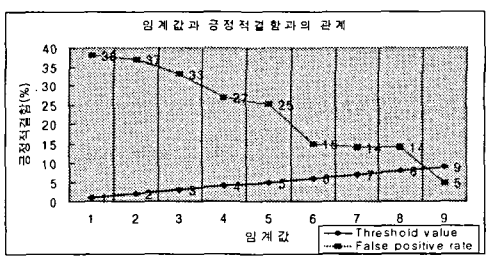

그림 6. 임계값과 긍정적 결함과의 관계

[그림6]에서와 같이 임계값을 증가시킬수록 긍정적 결함의 비율이 작아지는 것을 볼 수 있다. 하지만 9이상의 임계값을 주었을때는 긍정적 결함의 비율의 오차가 별 차이가 나타나지 않는다. 이것은 본 침입 탐지 시스템에서도 완벽하게 긍정적 결함을 없앨 수는 없다는 것이다. 그 이유는 감사데이터 학습과정에서 정상인 침입 패턴의 일부가 학습되어지기 때문에 완전하게 긍정적 결함을 제거하는 것은 불가능하였다.

V. 결론 및 향후 연구 방향

본 논문에서는 침입 탐지 시스템에 데이터마이닝 학습 기법을 도입하여 다량의 데이터 축약과 변형된 침입 패턴을 탐지할 수 있게 하였다.

특히 본 논문에서 제안한 시스템과 현재 사용되고 있는 다른 침입 탐지 방법들과 비교할 때, 탐지의 정확도를 높였고, 오판율을 줄이기 위해 임계값을 상황에 따라 조절하여 긍정적 결함을 최소화하였다. 본 시스템은 어떤 감사 데이터를 학습시키냐에 따라서 침입 탐지 범위가 결정된다. 따라서 다양한 감사 데이터 학습이나 감사 데이터 양에 따라 탐지 능력을 향상시킬 수 있다. 향후 연구 방향으로는 본 논문에서는 감사 데이터 학습 단계를 오프라인(offline)으로 처리하여 전체적인 시스템의 부하를 최소화하였으나, 온라인(online) 상태에서 수행하여 자동화된 침입 탐지 시스템을 구축하는 연구가 필요하다. 또한 감사 데이터 학습과정에서 최소 임계값을 결정하는 문제가 크게 대두되었다. 임계값을 크게 하면 수집된 데이터들에서 정확한 감사집합을 구하지 못해 부정적 결함(False negative)이 발생할 수 있다. 따라서 감사 데이터 학습 시 적절한 임계값 설정에 대한 연구가 필요하다.

참고문헌

[1] R. Buschkes, M. Borning, and D. Kesdogan, "Transaction based Anomaly Detection" Proc.of the Workshop on Intrusion Detection and Network monitoring, USENIX, Apr., 1999.

[2] Anup K. Ghosh, "Learning Program Behavior Profiles for Intrusion Detection", Proc. of the Workshop on Intrusion Detection and Network Monitoring, April., 1999.

[3] Samuel I. Schaen, "Network Auditing: Issues and Recommendations", IEEE 7th Computer Security Applications Conference, pp.66-79, Dec., 1991.

[4] T. Lane, "Filtering technique for rapid user classification", In Proceedings of the AAAI98/ ICML98 Joint Workshop on AI Approaches to Time series Analysis, 1998.

[5] U. Fayyad, G. Piatetsky-Shapiro and P. Smyth, "The KDD process of extracting useful knowledge from volumes of data", Communications of the ACM, 39(11):27-34, Nov., 1996.

[6] W. Lee, S. J. Stolfo and K. W. Mok, "Mining Audit data to build Intrusion Detection Models", In proceeding of the 4th International Conference on Knowledge Discovery and Data Mining, New York, NY, 1998.