디지털산업정보학회 논문지 제6권 제1호-2010년 3월

침입탐지시스템의 정확도 향상을 위한 개선된 데이터마이닝 방법론

최 윤 정*

Reinforcement Data Mining Method for Anomaly&Misuse Detection

Choi, Yun Jeong

〈Abstract〉

Recently, large amount of information in IDS(Intrusion Detection System) can be un manageable and also be mixed with false prediction error. In this paper, we propose a data mining methodology for IDS, which contains uncertainty based on training process and post-processing analysis additionally. Our system is trained to classify the existing attack for misuse detection, to detect the new attack pattern for anomaly detection, and to define border patter between attack and normal pattern. In experimental results show that our approach improve the performance against existing attacks and new attacks, from 0.62 to 0.84 about 35%.

Key Words : Intrusion Detection, Data Mining, Classification, Fault Tolerance System, SVM

Ⅰ. 서론

컴퓨터와 인터넷 인프라의 급속한 성장과 함께 정보시스템에 대한 불법적인 활용 시도가 늘어나며 네트워크 시스템의 오용 사례가 무서운 속도로 늘어나고 있다. 이러한 오용행위들은 시스템에 대한 단순한 호기심과 의도에서 시작했던 초창기 수준과 달리 위협적인 목적을 가진 공격적인 형태를 띠고 있으므로 피해로 인한 심각성이 매우 크다. 특정 서버의 취약점을 이용한 웜 바이러스에 의해서 일시적이지만 국가전체의 네트워크가 마비되는 사태가 일어나기도 했으며 주요 서버가 다운되는 사건이 발생하는 사건도 있었다[1]. 침입패턴들은 점점 새로운 형태의 이상 패턴들로 발전되어 불법적으로 범죄화되는 양상을 보이고 있다. 이러한 이상패턴들은 정상패턴들과의 구분이 명확하지 못하므로 사전에 미리 대처하기가 쉽지 않으므로, 이상패턴과 정상패턴을 모델링하는 연구가 필요하다. 또한 실제 침입패턴을 대상으로 한 실험이나 검증작업이 거의 희박한 상황에서 네트워크 공격도구에 의한 이상 침입패턴에 대한 연구는 매우 시급한 부분이기도 하다[2]. <표 1>은 인터넷에서 쉽게 구할 수 있는 대표적인 공격도구의 특징을 나타낸다. 이처럼 갈수록 지능화어가는 공격도구의 발전은 침입탐지시스템의 중요성을 가중시킨다.

최근 침입탐지시스템(Intrusion Detection System)에 데이터마이닝 기법을 적용하여 능동적인 침입탐지시스템을 구축하고자 하는 연구들이 활발하다. 데이터마이닝 기술은 대량의 데이터로부터 이전에는 알려지지 않은 의

* 서일대학 정보통신학과 교수(강의전담)

<표 1> 공격도구의 유형 및 특성

	Trinoo	Stacheldraht	Synk4
공격유형	UDP Flood	UDP/SYN/ICMP Flood, Smurf	SYN Flood
소스IP의 스푸핑	불가	자동 스푸핑	스푸핑 가능
소스타켓	지정 불가	자동선택 (랜덤/순차적)	자동선택 (랜덤)
타켓포트	지정 불가	범위지정 가능	범위지정 가능

미있는 유용한 정보를 추출하기 위한 기법으로 인공지능 분야의 기계학습이론과 정보이론, 통계, 시각화 기법을 통합한 기술이다[3]. 클러스터링, 분류, 연관규칙 등의 데이터마이닝 기법 등이 많이 적용되며, 이들을 구현하기 위한 알고리즘으로는 신경망, 유전자 알고리즘, 의사결정 트리 등이 있으며 침입탐지 분야에서 이상패턴과 사용자 행위를 설명하기 위한 특정 패턴을 추출하는 문제에 많이 적용되어 왔다. 대표적인 예로서 대량의 감사데이터를 효율적으로 분석하기 위해 자동화된 침입탐지모델을 구축하는 연구가 수행되었는데, 이를 위해서는 정상적인 프로파일이나 비정상적인 공격기법의 시나리오를 구축한 후 분류분석이 적용되었다. 이 후에도 실험 및 검증이 가능한 많은 양의 시스템과 네트워크 감사데이터를 통해 정확하고 효율적으로 분석해야 하는 일이 뒤따른다. 네트워크상에서 발생하는 다양한 형태의 대량의 데이터를 정확하고 효율적으로 분석하기 위해 설계되고 있는 마이닝 시스템들은 분석 목표 지향적으로 훈련데이터들을 어떻게 구축하여 다룰 것인지에 대한 문제보다는 대부분 얼마나 많은 데이터마이닝 기법을 지원하고 이를 적용할 수 있는지 등의 기법에 초점을 두고 있다. 최근의 공격기법을 탐지 및 차단하기 위한 방법은 에이전트화, 자동화 및 은닉화 된 공격 형태에 비해 미흡한 실정이다.

본 논문에서는 지능화된 침입패턴의 탐지를 위해 데이터마이닝 기법과 결함허용방법을 이용하는 개선된 학습알고리즘과 후처리방법에 의한 마이닝 프로세스를 제안한다. 본 논문에서의 설계한 시스템은 불확실성 기반의 향상된 후처리분석을 이용하며. 네트워크 내에서 발생가능 한 침입형태들을 분류한 결과를 재분석함으로써 정확성을 향상시키고 있다. 이는 기법에만 초점을 맞춘 기존의 데이터마이닝분석을 개선하고 있으며 특히 제안된 분석 프로세스를 진행하는 동안 능동학습방법의 장점을 수용하여 학습 효과는 높이며 분석비용을 감소시킬 수 있는 자가학습 방법의 효과를 기대할 수 있다. 이는 관리자의 개입을 최소화 하는 방법이면서 동시에 위양성(False Positive)와 위음성(False Negative)의 오류를 매우 효율적으로 개선하는 방법으로 기대된다.

본 논문은 다음과 같이 구성된다. 2장에서는 침입탐지 시스템의 구성요소와 여러 유형의 침입방안에 대한 내용을 정리하고, 3장에서는 이상탐지와 오용탐지의 성능을 높일 수 있는 개선된 데이터마이닝 방법을 제안한다. 4장에서는 이를 바탕으로 구현한 시스템과 실험내용을 정리하며 5장에서 결론을 맺는다.

Ⅱ. 관련연구

2.1 침입의 형태 및 방법

침입탐지시스템(IDS)은 분석 기법에 따라 이미 알려진 침입행위에 대한 정보를 이용하여 공격을 탐지해내는 오용탐지(Misuse Detection: action-based method) 와 사용자의 정상행위를 기반으로 정상적인 행동패턴 에 어긋나는 경우를 침입으로 탐지하는 이상탐지 혹은 비정상행위탐지(Anomaly Detection: profile-based method)로 나뉜다[2, 4-5]. 또한 이용하는 데이터 소스의 기반에 따라 호스트 기반과 네트워크 기반 방식으로 나눌 수 있다. 이들 시스템을 평가하는 기준들로는 기능성(Capability), 편의성(Usability), 성능의 우수성(Performance), 관리성(Manageability), 연동성(Inter-operability), 확장성(Scalability), 안정성(Robustness)등으로 규정되며, 이 중 무엇보다도 성능에 대한 중요성이 강조되는 상황이다[6].

1) 오용패턴 탐지

오용탐지 시스템은 침입탐지시스템에서 가장 일반적인 형태로서 오용행위가 발생되었을 때 빠른 시간 내에 탐지하고 복구하기 위한 목적의 분석이 이루어진다. 오용탐지는 이미 알려진 형태의 공격 순서를 시그너쳐(Signature)화하여 이 순서 혹은 특징을 따르는 상황을 공격이라고 판단한다. 알려진 공격방식 및 사이트별 보안정책과 같은 것을 규칙(Rule-Base)으로 구성하고 전문가 시스템을 활용하여 침입을 탐지한다.

<표 2>. 침입탐지의 정오분류표

		실제값	
		정상(1)	침입(0)
예측값	정상(1)	True Positive	False Positive
	침입(0)	False Negative	True Negative

민감도(sensitivity) = TP/ (TP+ FN)
특이도(specificity) = TN/ (TN + FP)
정확율(precision) = TP/(TP+FP)
재현율(recall) = TP/(TP+FN)

이는 일반적으로 알려진 공격에 대한 탐지능력만을 가지게 되므로 실제 침입이 아닌 경우 침입이라고 판정하는 위양성 오류가 비교적 적은데 반하여, 공격정보를 계속 수집해야 하며 알려진 공격 형태를 벗어나면 탐지할 수 없다는 한계점을 가지게 된다. 뛰어난 분석력 못지않은 예측력이 필요한 부분이다.

2) 이상패턴 탐지

오용패턴과 함께 또 다른 유형의 하나인 이상 탐지는 오랜 기간 축적된 정상적인 데이터를 수집하여 학습시킴으로써 정상적인 형태의 사용에 대한 프로파일을 완성한 후, 이와 다른 형태의 패턴을 가진 데이터를 탐지하는 방식이다. 즉, 정상 사용패턴을 모델링 한 후 이와 다른 변칙적인 행위가 있다면 오류로 탐지하는 방식이다. 기존에 알려져 있지 않은 침입을 탐지할 수 있고 실제의 침입을 침입이 아니라고 판정하는 위음성 오류를 줄일 가능성이 높다. 정상범위의 데이터 프로파일링을 통한 비정상행위 탐지기법에 대한 활발한 연구가 진행되고 있지만, 정상범위의 모든 데이터를 수집할 수 없다는 한계가 드러나며, 정상패턴과 공격패턴을 구분짓는데 있어서 많은 어려움이 존재하기도 한다[7]. 주로 사용자의 계정, 시스템파일 및 디렉토리 사용에 따른 변화들을 분석의 근거로 삼는다.

이와 비교할 수 있는 접근으로 정상적인 사용패턴을 학습시키는 대신 희귀한 패턴을 학습시키는 연구도 수행되었다. 미네소타 대학의 마인즈(MINesota INtrusion Detection System) 프로젝트는 희귀(Rare)한 패턴에서 학습데이터를 추출하여 분류를 위한 예측 모델을 생성하고 이상 패턴과 그 범위를 벗어나는 영역을 탐지하여 접근하는 방식의 연구를 수행한 바 있다[8]. 이상패턴에 대한 분석에 있어서 어느 관점과 어느 수준에서 보느냐에 따라 정상/이상으로 간주될 수 있기 때문에 근본적으로 트래픽 패턴의 이상여부를 검증한다는 것이 불가능할 수 있다. 따라서 위의 두 가지 탐지기법을 하이브리드방식으로 적용하는 연구가 활발하다[9-10].

2.2 기존 데이터마이닝에 의한 분석

통계적 방법을 이용한 공격 탐지 연구에서는 공격 도구에 의해 생성된 공격 패턴들은 정상 트래픽과 쉽게 구별되는 특징을 갖고 있으며 통계적인 기준을 이용하여 정상 트래픽과 공격 트래픽을 구별할 수 있다는 가정 하에 접근한다[11]. 실험을 위해 엔트로피와 카이제곱에 의한 통계방법이 주로 사용되며 정상 트래픽에서의 소스 주소의 분포와 공격 트래픽에서의 주소분포가 다르다는 점을 이용하여 탐지해 내고 있다. 반면, 나날이 지능화되어가는 공격 도구와 패턴들에 의하면 스푸핑의 랜덤정도가 조절가능하며 이로 인해 기존 가정을 재설정해야하

는 일이 필요하다. 따라서 단순히 소스 주소를 모니터링 하는 것으로는 공격 유형을 탐지 해내기 어렵다.

1) 연관규칙(Association Rule)

연관규칙은 항목집합으로 표현된 트랜잭션에서 각 항목간의 연관성을 반영하는 규칙으로서, 미리 주어진 최소 지지도와 신뢰도 값을 만족하는 항목집합들의 모든 집합들인 빈발항목집합을 찾아내어 연관규칙을 생성 한다[2, 9, 12-13]. 대량의 데이터로부터 적당한 특성이나 패턴 탐사를 위한 속성간의 연관성을 추출하며, 주로 감사 데이터(audit data)의 분석에 유용하여 많이 쓰인다. 연관규칙을 이용하여 침입 모델을 생성하여 시험한 [12]의 연구에서는 모델링에 드는 시간을 줄이기 위하여 학습과 탐지를 위한 에이전트를 구분한 침입탐지 시스템 구조를 제안하였다.

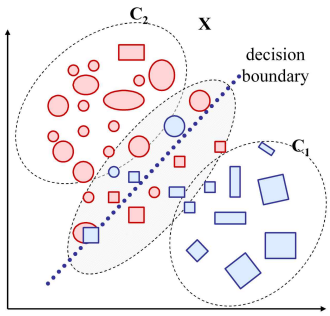
2) 분류(Classification)

분류란 데이터들을 미리 정해진 항목에 올바로 할당하는 것으로서, 각 항목에 대한 훈련데이터들의 학습을 통하여 분류규칙과 입력데이터를 비교하는 작업으로서 효율적인 정보관리 및 검색 등에 유용하다. 대부분의 문제들은 분류분석이 필수적인 만큼 분류분석의 성능향상을 위해 많은 연구가 진행되어 왔다. 기존의 분류성능 향상을 위한 연구들은 대부분 분류모델 자체를 개선시키는데 주력해왔으며 통계적인 방법으로 그 범위가 제한된다.

이원패턴인식 문제를 위해 제안된 SVM은 분류기법 중 가장 좋은 성능을 보이는 알고리즘 중 하나로, 뛰어난 인식성능을 바탕으로 침입탐지시스템에 많이 적용되었다. 또한 설명력이 약하다는 단점이 있으나 정확성이 높은 신경망(Neural Network) 알고지리즘을 이용하여 이상탐지와 오용탐지로 분류해 내는 연구도 제안되었다[10, 13-14].

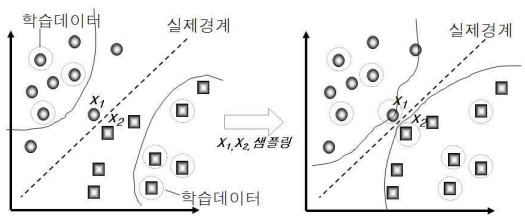
2.3 불확실성이 높은 데이터들의 분석을 위한 연구

불확실성이 높아 확실히 어느 항목으로 결정내리기 힘든 데이터들의 분류를 위한 연구로서, 능동학습이 제안되었다[15]. 이는 보다 유연하고 정교한 분석전략을 선택하기 위한 방법으로 데이터의 불확실성 개념을 이용한다. <그림 1>에서 나타내고 있듯이 데이터의 불확실성이 높으면 범주들의 경계선상에 있거나 경계영역에 근접해 있기 때문에 어느 범주로 구분되어야 할지 확실히 판단하기 힘든 성질을 지닌다.



<그림 1> 불확실성이 높아 분류경계에 인접해 있는 데이터들

<그림 2>은 능동적 학습알고리즘의 기본적 개념을 설명한다. 그림에서 ○와 □는 각각의 범주로 구분된 개체를 나타낸다. 이때 능동학습의 의미는 범주의 특징을 잘 설명하고 있는 정보력이 큰 데이터를 선택하여 학습시키는 것으로 이해할 수 있다.



<그림 2> 불확실성 기반의 샘플링 알고리즘의 개념

<그림 2>에서 초기 학습문서로 적당한 정보력이 큰 데이터는 좌표축에 가까이 위치한 데이터들이다. 반면, x1, x2 는 직관적으로 분류하기 어려운 불확실성이 높은 데이터들을 의미하는데, 초기에 정한 학습데이터들만 이용하면 x1, x2 와 같이 경계영역을 이루는 문서들은 분류기가 정한 경계와 멀어지게 되어 점점 더 분류되기 어려워진다. 이러한 데이터들을 처리하는 데 있어서 적절한 범주로 할당되게 하기 위하여 선택하여 학습시키는 것이 능동적 학습의 핵심이며, 학습집합 선택에 이러한 개념을 이용하는 것을 불확실성 기반 샘플링 알고리즘(Uncertainty based Sampling Algorithm)이라고 한다[15].

<그림 3>은 불확실한 문서들을 능동학습방법으로 샘플링하는 의사코드를 나타낸다.

<그림 2>의 □와 ○들을 예로 하여 정리하면 다음과 같다. 이들은 어느 범주로도 구분하기 힘든 불확실성이 높은 데이터이다. 이들이 많이 분포하면 경계선의 선형분리가 어려워 질 뿐 아니라 분류함수 생성에 대한 문제 이전에 불확실한 사례를 구별하기 위한 기준을 만드는 일부터 전문가의 적극적인 개입을 필요로 한다. 불확실한 개체들을 모두 학습데이터로 삼기 위해서는 각각의 내용을 개별 확인하여 지정해 주어야 하므로 일반적인 감독학습보다도 더 큰 학습비용이 든다. 게다가 모든 경계선상의 모든 개체들을 학습데이터로 삼다 보면 해당영역들의 자질들이 일반화되기 때문에 분류기준의 구분력이 상실되는 것이다.

이와 같이 경계면에 근접한 개체들을 처리하기 위해 최적의 결정 경계면을 찾는 분류알고리즘인 SVM은 최적화 방법이 가장 많이 연구되어 있다. SVM 분류기법에서는 위의 문제들에 대한 이상적인 하이퍼플레인을 찾아내면서 발생할 수 있는 문제에 대해 부분적인 오류허용 기법을 사용하고 있다[16].

Ⅲ. 불확실성 기반의 학습방법과 후처리분석에 의한 데이터마이닝 시스템

본 논문에서는 오분류 가능성이 높은 비정상 및 오용 데이터들의 개선된 분류분석을 통해 침입탐지시스템의 정확률을 높이고자 한다. 데이터의 복잡도 및 불확실성이 높으면 분류경계상의 위치가 명확하지 않고, 이는 <표 2>의 위양성, 위음성으로 나타나는 오분류율을 높이게 되어 분류결과의 신뢰도에 영향을 준다. 제안방법은 <그림 4>와 같이 분류목표에 따른 불확실성 기반의 학습시스템, 분류알고리즘의 적용, 그리고 분류결과의 후처리를 통해 침입여부를 결정하는 방법으로 구분되며 이에

1. Given Training Set : $(x_1, y_1), \ldots, (x_m, y_m)$ with m sample, Unlabeled data set X_u
2. D_t: **로부터 분류추정함수** h_t: ← $L(D_t)$
3. For t = 1, … m :
   - 3-a. X ← $U(X_u)$
     h_t:를 이용하여 X_u 로부터 가장 불확실성이 큰 데이터를 선택한다.
   - 3-b. **전문가가 데이터 x 에 라벨을 부여한다.** c_x ← c(x)
   - 3-c. **x를 학습집합에 추가한다.**
     D_t ← D_t {(x, c(x)) }
   - 3-d. **새로운 분류함수를 만든다.**
     h_t+1: ← $L(D_t)$
4. **마지막 분류함수** h_m+1 **을 최종 분류함수로 한다.**

<그림 3> 불확실성 기반 샘플링 알고리즘의 의사코드(pseudo code)

따라 학습과 후처리에 필요한 프로세스를 설계하였다.

3.1 불확실성 기반의 학습모델(ETOM)

1) 학습체계의 설정

학습의 효율을 높이기 위해서는 분류목표에 따른 학습체계가 설정되어야 한다. <그림 1>의 경우 기존방법은 경계선을 기준으로 뚜렷이 나누어지는 c1과 c2 이 필요할 것이다. 본 연구에서는 경계부근의 불확실성이 높은 데이터들의 분류를 위해 경계선 부근을 범주에 포함시켜 학습체계를 만든다. 학습데이터를 선택하는 문제에 있어 확실히 구분할 수 있는 c1과 c2 그리고 X영역의 데이터가 적당하다. 즉, 침입, 정상, 침입인지 정상인지 불확실한 데이터들이 각 영역의 학습데이터가 될 것이다.

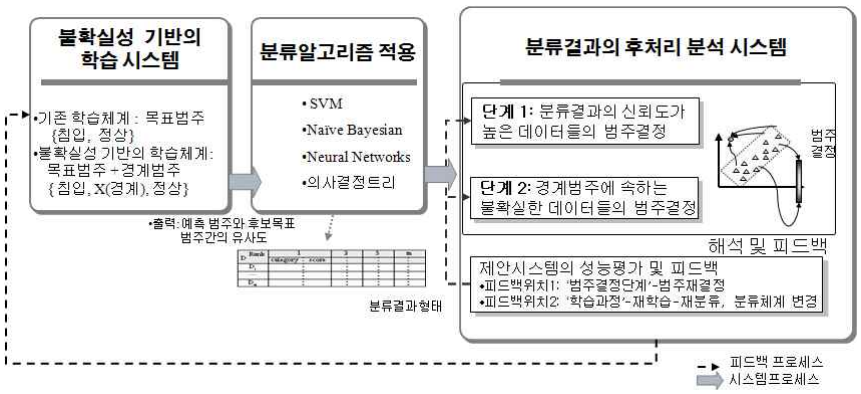
2) 클러스터링에 의한 경계영역 탐색

클러스터링은 개체의 유사도로 비감독학습하여 그룹을 형성하는 기법으로 개체의 특별한 정보가 없는 환경에서도 적용된다. 본 논문에서는 정보이론에서 자주 사용되는 엔트로피 개념을 이용하여 정보의 이상징후 여부를 판단한다. 엔트로피는 물질계의 열적상태를 나타내는 물리량으로 무질서도를 나타내는 지표로서 식 (1)과 같이 정의된다. 여기서 S는 s를 확률 변수로 갖는 집합을 의미하고 H(S)는 이 집합의 엔트로피, 그리고 P(s)는 s가 발생할 확률값을 의미한다. 엔트로피는 확률 변수에 대해 확률이 균등하게 분배되어 있을수록 큰 값을 가진다. 임의의 클러스터의 엔트로피가 낮을수록 내부 자질들의 유사도가 높은 좋은 클러스터임을 나타낸다.

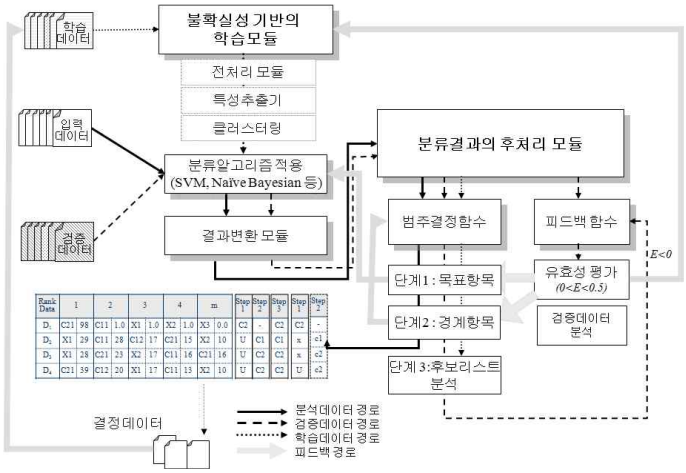
$$H(S) = -\sum_{s \in S} p(s) \log_2 p(s) \qquad (1)$$

실제 네트워크 환경에서는 이상징후가 정확히 정의되기 어려우므로 징후의 여부를 즉시 판단해 내기 위한 작업은 매우 추상적인 형태를 띤다. 특히 어느 수준까지를 이상 징후라고 판단해야 하는지 결정해야 하는 일은 전문가라 할지라도 쉽게 결정할 수 없는 문제에 속한다. 본 논문에서는 클러스터링 분석에 의해 분석 데이터에 대한 계획을 세운 후 공격 형태를 구체적으로 특성화하여 지도학습에 반영하고 있다.

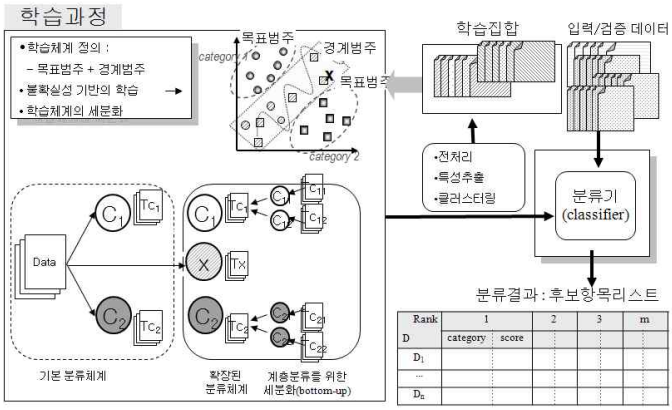
<그림 5>는 제안방법을 이용한 데이터마이닝 수행과정을 나타낸다. <그림 6>은 제안방법에 따른 학습형태를 나타낸다. 목표항목 C={침입패턴, X, 정상패턴}으로 정하고 이를 더 세분화 하여 목표항목 C={침입패턴, 침입에 가까운 패턴, X, 정상에 가까운 패턴, 정상패턴}으로 설정하여 각각에 해당하는 데이터로 학습시킨다. 이때 X는 구분하기 어려운 데이터, 즉 침입의 형태이나 정상패턴,



<그림 4> 향상된 학습과정과 후처리에 의한 데이터마이닝 시스템의 개요



<그림 5> 제안 시스템에서의 입출력 프로세스



<그림 6> 불확실성 기반의 학습 알고리즘 : 목표항목 vs. 목표항목+경계항목

혹은 정상적인 형태이나 침입패턴인 데이터이다. 이로 인해 기존의 C={침입, 정상}으로 학습했을 때보다 더 정교한 분류규칙을 얻을 수 있다.

3.2 분류결과의 후처리 분석 과정(RPOST)

위에서 정의한 분류체계에 의해 학습을 수행하고 분류 알고리즘을 적용하여 <그림 7>과 같은 전체 후보항목 리스트 L을 얻는다. 데이터 Di에 대한 후보항목리스트인 L_i는 범주와 점수치를 쌍으로 하는 순위 리스트이다.

L_i 에서 점수치는 적용한 분류알고리즘에 따라 상대적 혹은 절대적 수치값으로 얻어지며 데이터 D_i에 대한 L_i는 데이터와 범주들간의 유사도를 나타낸다고 볼 수 있다. 범주 할당작업은 분류수행 결과인 범주와 범주별 점수치 쌍인 이 랭킹정보를 분석하는 것이다. <그림 7>의 후보항목리스트의 분석에는 수치적 근거사항과 항목간 거리차를 이용한다.

<그림 8>은 분류결과가 모호한 즉, 1순위 범주가 X로 결정된 데이터들에 대해 수치적 특성과 항목의 거리차를 이용하여 의미상 가장 근접한 항목으로 할당시키는 알고

리즘을 나타낸다. 그림에서 쓰인 식 (2)~식 (4)를 설명하면 다음과 같다. 식 (2)에서 P는 피보트항목을 나타내며 X항목이 피보트가 된다. 식 (3)의 RD(P, l_{ij}. category)함수는 피보트항목 P의 순위와 l_{ij}. category의 순위격차를 의미하며 인접한 경우는 1이다. 후보항목내의 목표항목 c_i의 세부항목 c_{ik}들과 피보트항목간의 관련도는 목표항목 c_i로 합산시켜 궁극적인 목표항목 c_i로 지정한다.

$$Dist(P, c_n) = \sum_{j=1(l_{ij}.\text{category} \in c_n)}^{m} (RD(P, l_{ij.category}) * w_j) \quad (2)$$

$$RD(P, l_{ij.category}) = |P.rank - j| \quad (3)$$

$$w_r = \log(\sqrt{(r+\alpha)}) \quad (4)$$

α : control parameter

식 (4)의 w_r은 순위에 가중치를 부여하기 위한 함수로 r은 순위값이다. 이는 피보트항목과 비교되는 목표항목의 순위에 차이를 주기 위해 사용되었다. 사용자는 조절상수 α를 사용하여 순위별 가중치 값을 조정할 수 있다.

<그림 9>는 위의 결정방식에 따라서 피보트항목과 목표항목간의 거리를 근거로 한 지정방식을 보이고 있다. 예를 들어 <그림 9>의 2번 데이터가 범주 c2로 결정되는 과정은 다음과 같다.

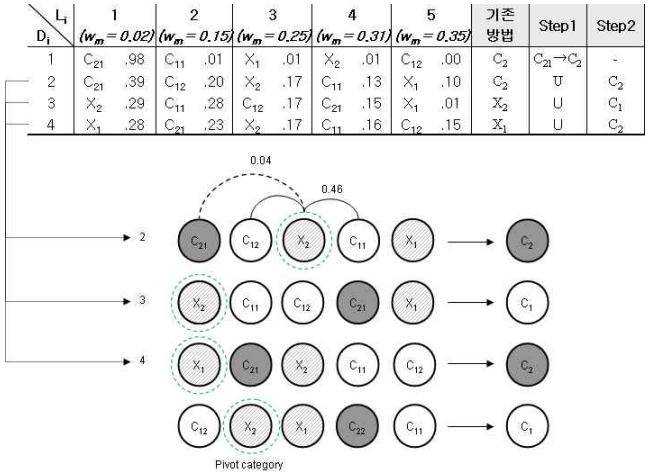
- 후보리스트내에서 가장 높은 순위의 경계항목을 찾아 피보트 항목으로 지정한다.
  → 2번 데이터에서는 x2가 선택됨.
- 후보리스트의 1순위부터 m까지 x2와 각 항목간의 거리를 식 (2)와 같이 계산한 후, 같은 목표항목간의 거리는 합산한다.
  → Dist(P, c2)=RD(x2, c21)*0.02=2*0.02=0.04,

<그림 7> 후보항목리스트(candidate category list)의 예

```
Input : 분류의 근거가 부족하여 X나 U로 분류된 문서들
N : 입력문서의 개수
n : 목표항목의 main index
m : window size
L[i]  : i= document
l[i][j]: i = document, j = rank

P= search_pivot(list)   # list 내에서 경계항목을 찾아 피보트로 지정하는 함수
# 후보항목리스트 Li에서 피보트 항목과 목표항목간의 거리계산
FOR  i = 1 to N {              # 문서 N개에 대하여
# 문서 i의 후보항목리스트 Li 에서 가장 높은 순위의 경계항목을 찾아 피보트항목으로 설정
   IF ((P= search_pivot(L[i]))  ≠  NULL)
   THEN  {                              # 문서 Di 의 후보항목리스트 Li 내에서
          FOR  j = 1 to m {            # 피보트항목 P 와 각 목표범주간의 distance 계산
               # cn  은 목표항목의 main index
                IF ( l[i][j]. category ∈ cn )
                THEN   Dist(P, cn )  +=  RD(P, l[i][j]. category) * wj
          }
          Li. step2  =  min{(Dist(P, cn )}      # 가장 가까운 목표항목으로 문서 Di 의 범주지정
   }
}
```

<그림 8> 후보항목리스트(candidate category list)의 수치분석을 위한 할당규칙



목표항목: c_1, c_2, 경계항목 : x_1, x_2,

<그림 9> 피보트 항목과 목표항목간의 관련도를 이용한 범주 결정 방법

Dist(P, c1)=RD(x2, c12)*0.15+RD(x2, c11)* 0.31
=1*0.15 + 1*0.31 = 0.46

- 2번 데이터의 범주는 Dist(P, c1) 과 Dist(P, c2)의 결과 중 보다 가까운 쪽의 목표항목으로 지정한다.
  → 범주 : c2 로 결정

이러한 과정을 통해 이전의 분류결과에서 발견하지 못했던 침입이나 정상오류를 다른 관점의 새로운 기준으로 재분석하는 것이 가능하여 좀 더 정확한 분류결과를 생성할 수 있다.

Ⅳ. 시스템 구현 및 실험

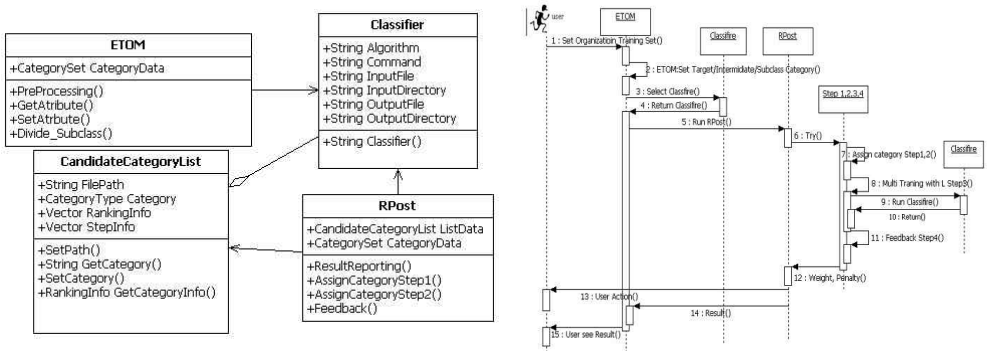
4.1 시스템 구현

본 논문에서 제안하는 침입탐지시스템은 <그림 4>와 <그림 5>와 같이 동작한다. <그림 10>은 제안방법의 구현을 위한 클래스 다이어그램과 시퀀스 다이어그램을 나타낸다. 여기서 학습모듈은 경계범주를 자동으로 탐색하여 학습체계를 설정하는 역할을 한다. 정상/침입에 대한 확실한 구분이 어려운 데이터들을 그룹핑하게 되는데, 데이터마이닝 프로세스상 분류알고리즘의 적용을 위한 전처리 역할을 하는 것이다. 본 논문에서는 분류성능이 가장 높다고 알려진 SVM을 적용하였다. 경계범주 탐색을 위한 클러스터링 분석을 위해 미네소타 대학에서 개발된 CLUTO-클러스터링 알고리즘을 적용하였으며, 인터페이스는 자바를 이용하여 구현하였다.

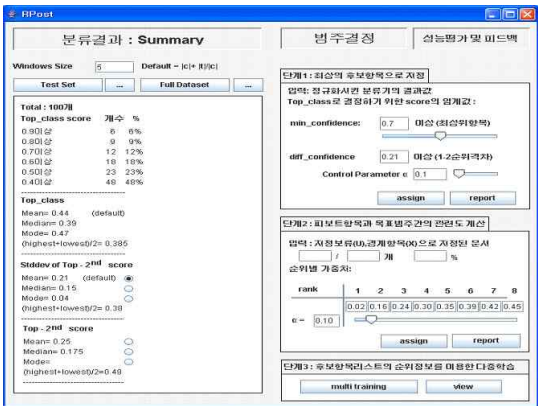
<그림 11>은 범주 결정과정을 시각화 한 후처리분석을 위한 메인 인터페이스로서, 화면 좌측에는 분류결과에 대한 전반적인 분석의 요약 정보를 나타낸다. 화면 우측에서는 이 정보를 바탕으로 임계값 및 조절변수들을 변경할 수 있고 그에 대한 변경된 결과를 동적으로 확인할 수 있도록 구현 하였다[17-18].

4.2 실험 및 평가

실험에 사용될 데이터는 실제 네트워크를 관리 툴인 시스코사의 NetFlow 툴을 이용하여 수집하였다. 5분마다의 플로우 정보를 이용하여 학습 및 평가를 위한 데이



<그림 10> 제안 시스템 설계를 위한 클래스 다이어그램과 시퀀스 다이어그램



<그림 11> 분류결과의 후처리 분석을 위한 구현 인터페이스

터로 이용하였다. 이 데이터는 기존의 실험에 사용되는 TCP덤프 데이터보다 많은 전처리과정을 생략할 수 있다. 분류분석을 수행하기 위한 테스트 데이터는 Snk4를 이용하여 발생시켰고, “Normal”, “Hard Normal”, “Hard Attack”, “Attack”의 레벨로 나누어 오분류율을 검사하였다. “Hard Normal”은 정상패턴으로 쉽게 구분이 되지않는 정상패턴을 말한다. 후보항목리스트에서 피보트와 목표항목간의 분석에 필요한 순위별 가중치 값은 순위별 격차를 조절을 위한 변수 α=0.1 로 하여 정하였다. 분류 알고리즘으로는 SVM을 적용하였다.

실험결과를 표로 나타내어 정리하면 다음과 같다. 표 3과 표 4를 바탕으로 표 5의 정확도(Accuracy)를 측정하였다. 정확율과 재현율 이외에도 정확도를 평가하는 기준으로 민감도 및 특이도를 함께 분석하는 경우가 종종 있는데, 예측된 결과와 실제 값이 다를 경우 위험도가 크고 판단기준의 신뢰도가 중요한 부분인 의학과 생물학 분야에서 많이 활용된다.

여기서 특이도의 의미는 실제 침입인 경우(음성)를 음성으로 옳게 예측해낸 비율을 나타내며, 민감도는 반대의 의미 즉, 양성으로 판정한 경우 중 실제 침입이 없는 (양성)것으로 옳게 예측해 냈는지의 비율을 나타낸다. 즉, ‘양성|음성’의 예측값과 실제값이 일치하는 정도를 평가한다. 이 값을 별도로 산출하여 분석하는 이유는 같은 정확도를 갖는다 하더라도 민감도와 특이도가 다를 수 있

<표 3> 기존 방법에 의한 정오분류표

		실제값	
		정상(1)	침입(0)
예측값	정상(1)	0.92	0.56
	침입(0)	0.53	0.87

<표 4> 제안 방법에 의한 정오분류표

		실제값	
		정상(1)	침입(0)
예측값	정상(1)	1	0.15
	침입(0)	0.21	0.98

<표 5> 기존방법과 제안방법의 정확도 비교

	민감도	특이도	정확율	F-Measure
기존방법	0.63	0.61	0.62	0.62
제안방법	0.82	0.87	0.87	0.84

으며, 경우에 따라서는 높은 민감도나 높은 특이도가 관건이 될 수 있기 때문이다. F-measure는 정확율과 재현율의 산술평균식인 2*(정확율*재현율)/(정확율+재현율)로 산출되고, 이진 분류의 경우 micro-averaged Breakeven Point는 (정확율 + 재현율)/2로 계산된다. 위 결과에 의하면 제안방법에 의해 침입을 옳게 예측한 특이도와 정상을 옳게 예측한 민감도가 각각 0.25, 0.19 향상되었음을 알 수 있으며 F-Measure값은 0.84로 기존방법보다 0.18 증가했음을 보인다.

V. 결론 및 향후연구

침입탐지시스템의 성능에 있어서 가장 중요한 요소는 탐지의 정확도이다. 특히 공격방법이 점점 다양화되고 지능화 되어가고 있는 상황에서 탐지력을 향상시키기 위한 연구는 매우 중요하다.

본 논문에서는 침입탐지를 위해 데이터마이닝 프로세스중 학습과 후처리 부분을 개선하였다. 일부 데이터마이닝에서는 신경망이나 유전자 알고리즘 같은 특정기법들에 초점을 두어 적용과정을 강조한다. 기존 데이터마이닝에 기반 한 침입탐지시스템 역시 다양하고 우수한 분석기법을 적용한다는 면에서는 의미가 있으나, 대부분의 경우 분석알고리즘 또는 기법선정에만 관심을 두고 있기 때문에 아쉬운 부분이 있었다. 본 논문에서는 다양한 지식탐사를 위한 개념적인 정보추출의 방법론이자 일련의 과정으로 이해해야 한다는 점을 강조하고 있다. 어떤 문제를 다루는데 정해진 기법이나 규칙이 정해져 있는 것이 아니라 데이터에 따라 혹은 다루어야 할 문제의 성격에 따라 다양한 기법들이 적용될 수 있어야 하기 때문이다. 데이터마이닝을 통해 얻어진 정보는 평가를 통해 다시 데이터마이닝 초기단계에 반영되고 재분석이 되면서 얻게 될 결과의 신뢰성을 높여가게 된다. 따라서 지침이 되는 가이드라인이 제시되어야하며 데이터마이닝 분석 후의 결과를 어떻게 활용할 것인가를 판단하는 인적요소의 역할 또한 중요하다. 이와 함께 우수한 훈련데이터와 강인하고 능동적인 학습과정 없이는 신뢰할만한 정확도를 얻기 힘들다는 것을 간과해서는 안 될 것이다.

본 논문에서의 제안방법은 학습데이터의 설정 및 훈련 방법을 개선함으로써 오분류율이 높은 침입패턴을 보다 정확히 발견해냄으로써 위양성/위음성 오류를 최소화하여 기존 방법에서 보다 약 35% 향상된 결과를 얻고 있다. 본 논문의 제안방법은 분석도구나 시스템에 의존하지 않기 때문에, 유사한 문제를 안고 있는 여러 분야의 네트워크 환경에 적용될 수 있을 것이다.

참고문헌

[1] D. Moore, G. M. Voelker, and S. Savage, “Inferring Internet Denial-of-Service Activity,” presented at USENIX Security symposium, 2001.

[2] 김정현, 안수한, 원유집, 이종문, 이은영, “마이닝을 이용한 이상트래픽 탐지 : 사례분석을 통한 접근,” 한국정보과학회 논문지, 정보통신, 제33권, 제 3호, 2006. 6

[3] 최윤정, 박승수, "학습방법개선과 후처리 분석을 이용한 자동문서분류의 성능향상 방법," 한국 정보처리학회논문지, 제12-B권, 제7호, 2005. 12, pp. 0811-0822.

[4] 엄남경, 우성희, 이상호, "SVM과 의사결정틀를 이용한 혼합형 침입탐지 모델," 한국 정보처리학회논문지, 제14-C권, 제1호, 2007. 2.

[5] 김병구, 정채명, "침입탐지 기술의 현황과 전망," 정보과학회지, 제18권, 제 1호, 2000, pp. 29~39.

[6] 유신근, 이남훈, 심영철, "침입탐지 시스템의 평가 방법론," 한국정보처리학회논문지, 제7권, 제11호, 2000. 11, pp. 3445-3460.

[7] Axelsson S., "The Base-rate Fallacy and the Difficulty of Intrusion Detection," ACM Transactions on Information and System Security, Vol. 3, No. 3, 2000, pp. 186-205.

[8] M. V. Joshi, R. C. Agarwal, V. Kumar, "Mining Needles in a Haystack: Classifying Rare Classed vis Two-Phase Rule Induction," ACM SIGMOD 2001.

[9] 김미희, 나현정, 채기준, 방효찬, 나중찬, "분산 서비스 거부 공격탐지를 위한 데이터마이닝 기법," 한국정보과학회 논문지, 정보통신, 제 32권 제 3호, 2005. 6.

[10] A. K. Ghosh, A. Schwartzbard, "A Study in using Neural Networks for Anomaly and Misuse Detection," In Proc. of the 8th USENIX Security Symposium, Washington, D. C., USA, Aug. 1999

[11] L. Feinstein, D. Schnackenberg, R. Balupari, D. Kindred, "Statistical Approaches to DDoS Attack Detection and Response," n Proc. of the DARPA Information Survivability Conference and Exposition, 2003

[12] Wenke Lee, et al., "Data Mining Approaches for Intrusion Detection," In proceedings of the 7th USENIX Security Symposium, SanAntonio, TX, 1, 1998.

[13] Wenke Lee, et al., "Mining Audit Data to Build Intrusion Detection Models," In proceedings of the 4th International Conference on Knowledge Discovery and DataMining, NewYork, 8, 1998.

[14] 박명언, 김동국, 노봉남, "가우시안 혼합모델을 이용한 네트워크 침입탐지시스템," 한국 정보과학회, 제32회 추계학술발표회 논문집, 제 32권 제 2호

[15] D. Koller and S. Tong, "Active Learning for Parameter Estimation in Bayesian Network," In Neural Information Processing System, 2001

[16] T. Joachims, "Making Large-Scale SVM Learning Practical," In Advanced Kernel Method-support Vector Learning, MIT Press, 1999

[17] 최윤정, "ETOM+RPost기반의 문서분류시스템의 설계 및 구현," 한국 산학기술학회논문지, 제11권, 제2호, 2010. 2

[18] 최윤정, 박승수, "경계범주 자동탐색에 의한 확장된 학습체계 구성방법," 한국 정보처리학회 논문지, 제6-B권, 제6호, 2009. 12, pp. 471~480.

■ 저자소개 ■

최 윤 정
Choi, Yun Jeong

2009년 3월~현재 서일대학교 정보통신과 강의전담
2007년~2008년 서강대학교 컴퓨터학과 Post. Doc
2007년 2월 이화여자대학교 컴퓨터공학과 (공학박사)
2001년 8월 이화여자대학교 컴퓨터공학과 (공학석사)
1997년 2월 서원대학교 전자계산학과(이학사)

관심분야 : 인공지능, 기계학습, 온톨로지, 상황정보인식, 유비쿼터스, 센서네트워크
E-mail : cris@seoil.ac.kr

논문접수일 : 2009년 11월 5일
수 정 일 : 2010년 2월 10일
게재확정일 : 2010년 2월 20일