SVM과 데이터마이닝을 이용한 혼합형 침입 탐지 모델

The Model using SVM and Decision Tree for Intrusion Detection

엄남경[1], 우성희[2], 이상호[1]

[1] 충북대학교 전자계산학과
E-mail: {family, shlee}@chungbuk.ac.kr
[2] 충주대학교 멀티미디어학과
E-mail: shwoo@cjnc.ac.kr

요 약

안전한 네트워크를 운영하기 위해, 네트워크 침입 탐지에서 오탐지율은 줄이고 정탐지율을 높이는 것은 매우 중요한 일이다. 최근 얼굴 인식, 생물학 정보칩 분류 등에서 활발히 적용 연구되는 SVM을 침입탐지에 이용하면 실시간 탐지가 가능하므로 탐지율의 향상을 기대할 수 있다. 그러나 입력 값들을 벡터공간에 나타낸 후 계산된 값을 근거로 분류하므로, SVM만으로는 이산형의 데이터는 입력 정보로 사용할 수 없다는 단점을 가지고 있다. 따라서 이 논문에서는 데이터마이닝의 의사결정트리를 SVM에 결합시킨 침입 탐지 모델을 제안하고 이에 대한 성능을 평가한 결과 기존 방식에 비해 침입 탐지율, F-P오류율, F-N오류율에 있어 각각 5.6%, 0.16%, 0.82% 향상이 있음을 보였다.

키워드 : SVM, 침입 탐지 시스템(IDS), 데이터마이닝, 의사결정트리

1. 서 론

오늘날 컴퓨터와 통신 기술의 급속한 진전은 각종 정보를 공유하게 하였지만, 역기능으로써 정보의 위조나 변조 또는 허락 없이 유출되는 불법 행위가 발생되는 등 폐해 또한 심각하다.

침입 방지 기술이나 IDS(Intrusion Detection System) 기술은 꾸준히 발전하고 있으며, 이진 분류 능력이 뛰어난 SVM(Support Vector Machines)을 이용한 효율적인 연구가 행해지고 있다. 그러나 SVM은 입력 값을 벡터 공간에 나타낸 후 계산된 값을 근거로 분류를 수행하므로 벡터 값으로 표현이 불가능한 연속형 데이터는 취급할 수 없다[1]. 따라서 이 논문에서는 기존의 SVM 기반의 침입탐지 시스템에서 입력정보로 사용하지 못했던 이산형(Discrete type)의 데이터를 의사결정트리 방법을 이용하여 추가적으로 탐지함으로써 침입 탐지율을 향상시키는 모델을 제안하고자 한다.

2. 관련 연구

2.1 SVM을 적용한 침입 탐지

SVM은 1995년 Vladimir Vapnik에 의해 이원 패턴 인식 문제를 해결하기 위해 제안된 학습 방법으로 부정 예제로부터 긍정 예제를 분류해 낼 수 있는 결정면(Hyperplane)을 찾아내는 분류 모형이다[1]. 이진 레이블을 목표 변수로 갖는 데이터의 분류작업에 있어서 매우 좋은 성능을 보이는 SVM은 명료한 이론적 근거와 뛰어난 인식 성능을 바탕으로 SVM 기반의 IDS들은 시스템에 입력되는 특징들의 수를 줄임으로써 문제를 간결하게 하며, 침입 판정 시간을 줄일 수 있고, 침입 탐지 결과의 정확성을 높일 수 있다

[2][3].

2.2 데이터마이닝을 적용한 침입 탐지

데이터마이닝은 데이터베이스에 존재하는 방대한 양의 자료로부터 사전에 알려지지 않은 암시적이고 유용한 정보를 추출하는 것으로 인공지능 분야의 기계학습 이론에 그 뿌리를 두고 있다. 침입 탐지 분야에서의 데이터마이닝 기법은 프로그램과 사용자 행위를 설명하는데 필요한 특징 패턴을 추출하는 등에 사용된다. 이 과정에서 결과에 대한 유용성과 불확실성을 정량화 할 수 있게 되며, 수행 결과로 패턴이나 새로운 정보를 얻게 된다[4].

의사결정트리의 하나인 C4.5와 신경망 모델을 결합한 하이브리드 방식의 침입 탐지 모델은 신경망과 C4.5 알고리즘이 분류할 수 있는 공격이 다르다는 점을 이용하여 둘의 방식을 결합한 모델로 서로의 장점을 이용하면 침입 탐지율을 높일 수 있다[5].

3. SVM과 데이터마이닝 결합 침입탐지 모델

3.1 제안 모델의 개요

이 논문에서 제안하는 침입 탐지 모델의 프레임워크는 (그림 1)과 같다. 제안 모델의 프레임워크는 크게 탐지 모듈과 학습 모듈로 나누어진다. 학습 모듈에서는 침입 감사데이터를 이용하여 SVM과 데이터마이닝 학습이 이루어지고 탐지 모듈에서는 학습 모듈의 학습 결과를 바탕으로 침입 탐지를 수행한다.

<표 1>에서 연속형 데이터와 이산형 데이터의 예를 보인다.

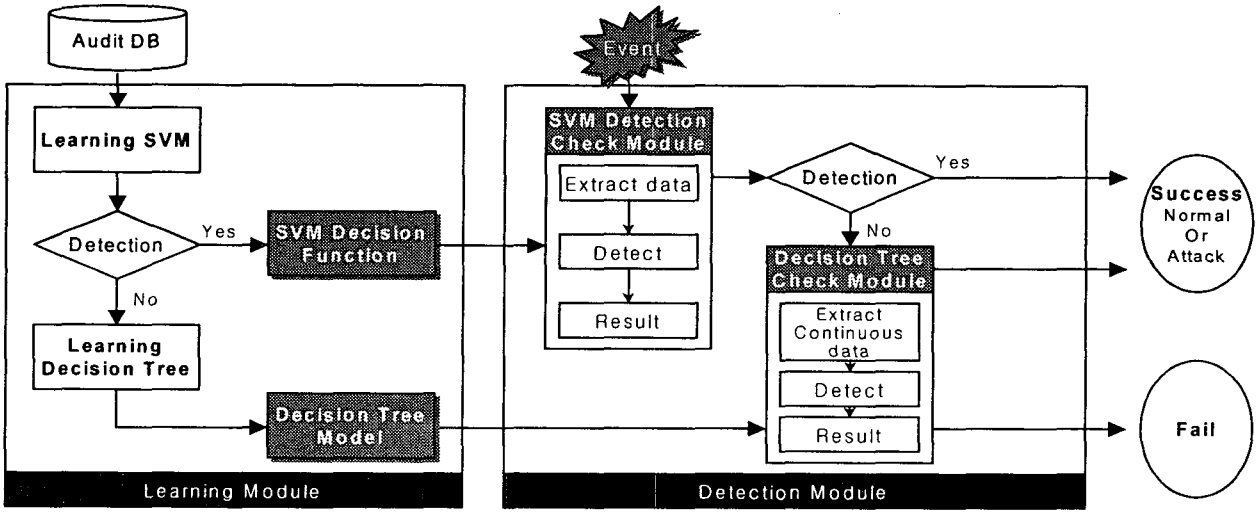
<표 1> 연속형/이산형 데이터의 예

데이터 타입	데이터 속성	특징 설명
연속형	duration	연결시간
	src_bytes	소스로부터의 데이터길이
	urgent	Urgent 패킷 개수
	hot	"Hot" indicator 개수
	num_root	root 접근 회수
	num_access_files	파일 접근 회수
	num_failed_logins	로그 실패 회수
이산형	protocol type	프로토콜 타입(TCP, UDP등)
	service	서비스 종류(HTTP, FTP등)
	flag	정상 또는 에러 플래그
	land	1:같은 소스/목적지 주소, 0
	logged_in	로그 성공/실패 여부
	root_shell	1:root shell 획득, 0
	su_attampted	1:" su root"명령 시도, 0

3.2 학습 모듈

3.2.1 SVM 학습 모듈

SVM 학습은 침입과 정상을 구분할 수 있는 서포터 벡터와 가중치 벡터 값으로 이루어지는



(그림 1) 제안 프레임워크

결정함수를 구하는 과정이다. 학습과정을 통해 입력 벡터 값에 따라 고차원 공간에 침입과 정상을 구분할 수 있는 최대 마진을 가지는 결정면을 가진다.

3.2.2 의사결정 트리 학습 모듈

의사결정트리는 많은 컴퓨팅 작업 없이 분류 과정을 형성하며 이산형 변수와 연속형 변수에 모두 사용할 수 있다. 때문에 SVM 학습 결과 탐지하지 못한 데이터의 이산형 데이터 부분만을 추출하여 의사결정트리 방법을 적용한다.

3.3. 탐지 모듈

3.3.1 SVM 탐지 모듈

SVM 탐지 모듈은 SVM 학습을 통해 생성된 결정함수에 침입 감사 데이터를 적용하여 침입 여부를 판정하는 모듈이다.

3.3.2 의사결정트리 탐지 모듈

의사결정트리 탐지 모듈은 의사결정트리 학습을 통해 생성된 모델에 SVM 탐지 모듈에서 탐지하지 못한 데이터만을 적용하여 침입을 판정하는 모듈이다.

4. 실험 및 평가

4.1 실험 환경

각각의 연결기록은 41개의 독립적인 속성과 공격 유형 레이블로 이루어져 있으며 상세한 데이터 구성은 [표 2]와 같다.

<표 2> KDD Cup 99 데이터 셋의 구성

항 목		개 수
총 데이터 수		311,029
총 속성의 수	이산형	9
	연속형	32
	공격 유형 레이블	1
	합계	42
공격유형 클래스		4
총 공격 유형		38

IDS는 탐지대상으로부터 생성되는 시스템 사용 내역, 컴퓨터 통신에 사용되는 패킷 등과 같은 데이터를 수집하는 침입 감사 데이터(Audit Data) 수집 과정을 거친다. 이후 수집 된 침입 감사 데이터는 침입 판정이 가능할 수 있도록 데이터 가공 및 축약(Data Reduction and Filtering) 과정을 거쳐 의미 있는 정보로 전환 된다. 이렇게 생성된 침입 감사 데이터는 SVM에 입력되기 전에 SVM 머신의 표준 입력 형식에 합당하도록 포맷을 변환하여야 한다.

4.2 성능 평가 기준

제안 방법의 성능을 평가하기 위한 항목으로 탐지율과 False Positive 오판율, False Negative 오판율을 사용하며 계산방법은 다음과 같다.

$$\text{탐지율} = \frac{\text{시스템에 의해 침입으로 판정된 침입 데이터의 개수}}{\text{전체 침입 데이터 개수}} \times 100 \quad \text{식-①}$$

$$\text{F-P오류율} = \frac{\text{시스템에 의해 침입으로 오판된 정상 데이터의 개수}}{\text{전체 정상 데이터 개수}} \times 100 \quad \text{식-②}$$

$$\text{F-N오류율} = \frac{\text{시스템에 의해 정상으로 오판된 침입 데이터의 개수}}{\text{전체 침입 데이터 개수}} \times 100 \quad \text{식-③}$$

식-①은 탐지율로써 전체 침입 데이터 중 시스템에 의해 침입으로 정확히 판정된 데이터의 비율을 백분율로 나타낸 값이다. 식-②는 False Positive 오판율로 전체 정상 데이터 중 시스템에 의해 침입으로 오 판정된 데이터의 비율을 백분율로 나타낸 값이며, 식-③은 False Negative 오판율로 전체 침입 데이터 중 시스템에 의해 정상으로 오 판정된 데이터의 비율을 백분율로 나타낸 값이다.

4.4. 평가

<표 3> 기존 모델의 탐지 실험 결과

실험 / 평가척도	실험 1	실험 2	실험 3	평균
학습 시간	45분 45초			45분45초
탐지소요시간	29분 30초	31분 19초	31분 6초	30분 39초
탐지율	92.01%	92.90%	92.89%	92.60%
F-P오류율	3.03%	3.07%	3.01%	3.03%
F-N오류율	9.02%	9.09%	9.09%	9.06%

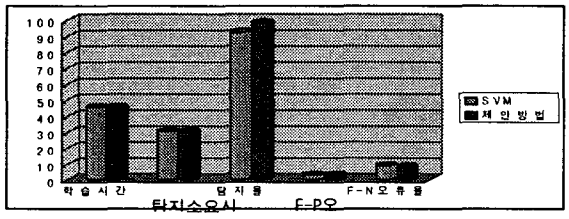
<표 4> 제안 모델의 탐지 실험 결과

실험 / 평가척도	실험 1	실험 2	실험 3	평균
학습 시간	45분 47초			45분 47초
탐지소요시간	29분 39초	31분 28초	31분 16초	30분 39초
탐지율	97.76 %	98.35 %	98.78 %	98.20 %
F-P오류율	2.88%	2.93%	2.81%	2.87%
F-N오류율	8.29%	8.21%	8.22%	8.24%

<표 5>는 기존 방법과 제안 방법의 실험 결과이며, (그림 2)는 SVM과 제안방식을 비교한 그래프이다.

<표 5> 제안 방법과 기존 방법의 성능 비교

평가기준 / 방법	학습 소요시간	탐지 소요시간	탐지율	F-P 오류율	F-N 오류율
SVM	45분 45초	30분 39초	92.60%	3.03%	9.06%
제안방법	45분 47초	30분 48초	98.20%	2.87%	8.24%



(그림 2) SVM과 제안방식 비교

실험 데이터 100건당 학습에 소요된 시간은 2.747초, 탐지에 소요된 시간은 1.848초이며 전체 학습에 추가로 소요된 시간은 2초, 탐지 실험에 추가로 소요된 시간은 9초로 제안 방법에 추가로 소요된 시간은 전체 학습, 탐지시간에 미치는 영향이 미미하다.

5. 결론

기존의 SVM을 이용한 IDS에서는 SVM의 입력 정보로 연속형 데이터만을 고려하여 학습과 실험을 수행하였다. 그러나 SVM에 입력으로 사용될 수 없었던 이산형 데이터는 침입 판정에 상당한 영향을 미치는 중요한 정보들을 포함하고 있다. 따라서 이 논문에서는 침입을 탐지하는데 있어 분류능력이 탁월한 SVM과 이산형 데이터를 입력 정보로 사용하여 동작이 가능한 데이터마이닝 기법을 결합하여 침입을 탐지하는 모델을 제안하고 실험 하였다. 향후 연구로는 학습 시간과 탐지 시간을 줄이기 위해 탐지에 적합하면서도 많은 시간을 요구하지 않도록 학습 데이터양을 조절하는 연구가 필요하며, 실시간 탐지를 만족시키기 위한 연구와 실험도 병행되어야 하겠다.

참 고 문 헌

[1] An Introduction to Support Vector Machines and Other Kernel-Based Learning Methods, N. Cristianini an, J. Shawe-Taylor, Cambridge University Press, 2000

[2] Identifying important features for intrusion detection using support vector machines and neural networks, Sung, A.H. Mukkamala, S., Applications and the Internet, 2003. Proceedings. 2003 Symposium on , 27-31 Jan. 2003

[3] One-Class Training for Masquerade Detection, Ke Wang, Salvatore J. Stolfo, CU Tech Report April 2003

[4] Data Mining Framework for Building Intrusion Detection Models, Wenke Lee, Salvatore J. Stolfo, Kui Mok, In Proceedings of the 1999 IEEE Symposium on Security and Privacy, Oakland, CA, May 1999

[5] Hybrid neural network and C4.5 for misuse detection, Zhi-Song Pan; Song-Can Chen; Gen-Bao Hu; Dao-Qiang Zhang, Machine Learning and Cybernetics, 2003 International Conference on , Volume: 4 , 2-5 Nov. 2003 Pages:2463 - 2467 Vol.4