SVM classification을 이용한 호스트 기반 침입 탐지

이주이, 김동성, 박종서, 염동복

한국항공대학교 컴퓨터공학과

Detecting Host-based Intrusion with SVM classification

Julee Lee, Dong-seong Kim, Jong-sou Park, Dong-bok Yeom

Department of Computer Engineering Hankuk Aviation Univ.

요 약

본 연구에서는 Support Vector Machine(SVM)을 이용한 호스트 기반 침입 탐지 방법을 제안한다. 침입 탐지는 침입과 정상을 판단하는 이진분류 문제이므로 이진분류에 뛰어난 성능을 발휘하는 SVM을 이용하여 침입 탐지 시스템을 구현하였다. 먼저 감사자료를 system call level에서 분석한 후, sliding window기법에 의해 패턴 feature를 추출하고 training set을 구성하였다. 여기에 SVM을 적용하여 decision model을 생성하였고, 이에 대한 판정 테스트 결과 90% 이상의 높은 침입탐지 적중률을 보였다.

I. 서론

인터넷이 발달하고 네트워크를 통하여 자유롭게 정보가 이동됨에 따라 침입이 증가하고 있다. 이러한 침입에 대하여 실시간으로 탐지하고 적절한 조치를 취하는 방법으로 침입 탐지는 그 중요성을 더해가고 있다. 침입 탐지는 침입을 판단하는 감사자료의 출처에 따라 네트워크 기반의 침입 탐지와 호스트 기반의 침입탐지로 나누어지며[1], 호스트 기반의 침입 탐지는 네트워 기반의 침입 탐지에 비해 복잡하고 알려지지 않은 공격을 탐지하는데 효과적이다. 침입 탐지는 침입 탐지 모델에 따라 오용 탐지와 비정상 탐지로 나누어진다. 오용 탐지는 이미 알려진 침입 패턴을 토대로 침입을 탐지하는 기법이다. 이를 이용한 방법에는 전문가 시스템, 상태 전이 분석, KeyStroke 분석 등이 있다[2]. 오용탐지는 정확한 침입 탐지가 가능하고 구현하기도 비교적 쉬우며, 비교적 빠른 속도로 구현할 수 있다. 그러나 단지 정의된 침입 패턴만 탐지가 가능하고 새로운 공격에 대해서 rule update후에 탐지할 수 있으므로 대응이 늦다. 이에 반해 비정상 탐지는 사용자의 정상적인 행위를 분석하여 비정상 행위를 통계적으로 판단하는 침입 탐지 방법이다[3]. 사용자의 정상적인 행동을 모델링 한 후 사용자의 행위가 정상적인 행동에서 얼마나 벗어났는지를 측정하고 임계치를 초과하면 그 행위를 침입 행위로 판단한다. 이 탐지 방법은 오탐지율이 높다. 또한 많은 통계적인 계산을 필요로 하므로 비용이 높고 구현하기도 어렵다. 그러나 알려지지 않은 침입을 탐지하는데 효과적이다.

본 논문에서는 이러한 오용탐지와 비정상 탐지의 문제점을 개선하기 위해 Support Vector Machine(SVM)을 이용하여 호스트 기반의 침입 탐지 방법을 제안하고 실험하였다. SVM은 1995년 Vapnik에 의해 제기된 학습 알고리즘으로 복잡한 패턴 인식, 분류 문제에 뛰어난 성능을 발휘하여S문자, 얼굴, 그리고 물체 인식 등의 실제분야에 성공적으로 적용되었고, 특히 이진분류문제를 최적으로 해결한다[4]. SVM은 top-down으로 접근하는 학습방법으로 기존의 bottom-up 방식의 여러 학습 방법보다 계산량이 적어 속도가 빠르며 대용량의 데이터에 대해서도 처리할 수 있다[5]. 또한 동적으로 트레이닝 패턴을 갱신할 수 있는 기능을 제공한다. 본 실험에서는 사용자의 행위 패턴과 침입 패턴을 training set으로 구성하였고 이로 인해 알려진 침입 패턴 뿐만 아니라 알려지지 않은 침입 패턴에 대해서도 탐지할 수 있다는 장점이 있다.

본 논문은 과학기술부.한국과학재단 지정 경기도 지역협력연구센터(RRC)인 한국항공대학교 인터넷정보검색연구센터의 지원에 의한 것입니다.

본 논문의 구성은 다음과 같다. 먼저 2절에서는 SVM에 대하여 간략하게 설명하고, 3절에서는 제안하는 침입 탐지 방법으로 SVM을 이용한 침입 탐지 대하여 설명한다. 다음으로 4절에서는 제안하는 방법을 이용한 실험에 대하여 설명하고, 마지막으로 5절에서 향후 연구 방향을 언급하며 결론을 맺는다.

II. Support Vector Machine

SVM은 Vladimir Vapnik에 의해 고안되었으며, classification 문제를 해결하기 위해서 최적 분리 경계면을 제공한다.[4] SVM은 입력 벡터로 training data를 받아들여 고차원 공간의 위치로 nonlinear mapping을 한다. 그리고 이 고차원 공간에서 최적의 분류를 위한 초평면을 찾아내고 이것을 기준으로 테스트를 시행하여 분류 결과를 얻는다. 이 때 최적 분리 경계면을 결정하는 초평면 결정함수는 수식(1)과 같다.

$$D(x) = (\vec{w} \cdot \vec{x}) + b \quad (1)$$

이 식에서 $\vec{w}$는 각각의 입력에 대한 가중치 벡터를 나타내며, b는 경계값을 나타낸다. 그림 1은 geometric view에서 SVM classification을 나타낸 것이다. 최적 분리 경계면에서 가장 근접한 입력 벡터를 support vector라고 하며, support vector를 포함하는 초평면 사이의 거리인 margin 값을 클수록 분류 성능이 더 좋아진다. 즉, SVM은 학습 패턴이 주어질 때, margin 값을 최대로 하는 최적 분리 경계면 가중치 벡터와 경계값 을 찾는 최적화 문제로 생각할 수 있다.

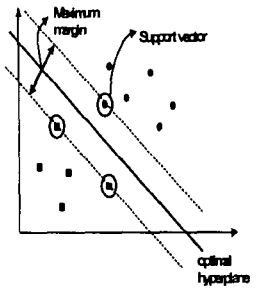

그림 1.geometric view에서 SVM classification

III. SVM을 이용한 침입탐지 방법

비정상 탐지에서 침입 판단의 문제는 데이터를 침입과 정상의 두 가지로 분류하는 이진 분류의 문제로 볼 수 있다[6]. 따라서 IDS에서 침입을 판단하기 방법으로 통계적인 학습 도구인 SVM을 이용하였다. SVM 기반의 침입 탐지는 이미 알려진 침입과 정상 데이터를 수집하여 학습시킨 후에 학습에 사용되지 않은 일부 데이터를 시험하여 정확도 면에서 성능을 측정해 볼 수 있다. 그림 2는 Two-class SVM 기반 침입 탐지 모델의 구성요소이다.

감사 자료 수집: 기계 학습에 의한 침입 탐지 모델을 구현하기 위하여, 먼저 침입 탐지의 근거 자료가 되는 감사 자료를 수집한다. 본 연구에서는 특권 프로세스에서 발생하는 system call trace를 감사자료로 채택하고, sendmail bug에 대한 system call trace set을 사용하였다[7, 8].

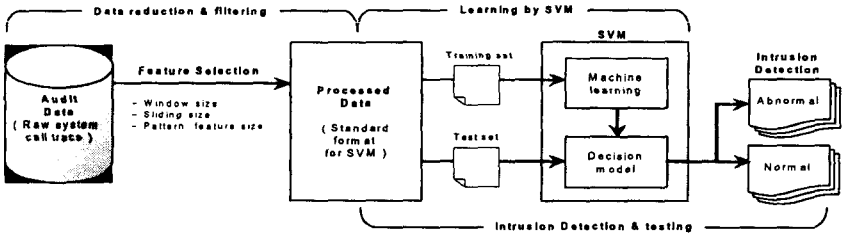

그림2: Two-class SVM 기반의 침입 탐지 모델 구성요소

Sendmail은 특권 프로세스 하에서 동작하는 프로그램이며, 알려진 취약성이 많고 현재에도 많은 취약점들이 보고되고 있다[18]. 또한 변화하는 다양한 정상 system call traces를 충분히 정의할 수 있다[8].

자료 축약 및 추출: 수집한 감사자료를 그대로 사용하기에는 그 정보가 너무 방대하고 실제 시스템에 적용하기 쉽지 않다. 따라서 대량의 원시 자료에서 의미 있는 정보를 추출해야 한다. 본 연구에서는 의미 있는 정보를 추출하기 위한 data mining기법으로[9] sliding window의 개념을 적용하여 window size의 패턴을 찾고, 반복적인 패턴의 빈도수를 기준으로 패턴을 선택한다. 각 trace마다 선택된 패턴들은 그 trace의 feature가 되며, window size와 sliding size, 그리고 pattern feature size를 변화시키면서 다양하게 data set을 구성한다. 구성된 data set은 다시 SVM을 적용하기 위해 알맞은 형식으로 가공된다.

SVM에 의한 학습: SVM learning을 위해서 가공된 data set으로부터 training set을 구성한다. Window size와 sliding size, 그리고 pattern feature size의 변화에 따라 다시 training set을 구성하고 반복적인 트레이닝을 하여, 정상과 침입을 분류하기 위한 decision model을 생성한다.

결과분석 및 침입탐지: 반복적인 트레이닝의 결과로 만들어진 SVM 기반의 decision model에 테스트를 시행하고, 그 결과의 분석을 통하여 침입 탐지율이 높게 나타나는 decision model을 찾는다. 즉 이러한 반복적인 과정을 통해서 정상과 침입을 분류하는 최적의 분리 경계 면과 이 때의 window size와 sliding size, 그리고 pattern feature size 찾을 수 있다.

IV. 사례 연구

우리는 제안된 방법에 대한 실험을 위하여, 가장 일반적인 침입중의 하나인 sendmail에 관한 알려진 침입과 정상의 system call trace를 수집하고, training set과 test set을 구성하여 실험하였다. 실험은 수집된 원시 자료로부터 특징이 되는 자료를 추출하는 data preprocessing 단계와 추출된 data set에 SVM으로 적용하여 침입과 정상을 판단하는 classification단계로 이루어진다.

1. Data Preprocessing

Data Preprocessing 단계에서는 먼저 sendmail에 관한 알려진 침입과 정상 system call trace를 수집하여 원시 data set을 구성하고, 이로부터 의미 있는 데이터를 추출한 후, SVM classification을 적용하기 위하여 적절한 형식으로 다시 가공한다.

먼저 sendmail에 관한 정상과 침입 system call trace 각각 14 case를 New Mexico대학의 공개 database로부터 수집하여[10,11], 원시 data set을 구성한다. 다음으로 수집한 system call trace에 대하여 윈도우를 슬라이딩하면서 윈도우 크기의 패턴을 찾고, 찾은 패턴의 빈도 수를 계산하여, 빈도 수가 높은 상위 일정 수만을 그 trace의 feature로 선택하였다. Data preprocessing을 위한 마지막 작업으로, 추출된 feature data set을 SVM classification에 적합한 형식으로 재구성한다. 이 때, 각 feature 값이 나타내는 것은 추출된 패턴과 일대일로 매핑된 값이다.

2. Classification and Testing

Data preprocessing 단계에서 구해진 Normal, abnormal case 각각에 대하여 case 1~9는 training set으로, case 10~14는 test set으로 구성하였다. 이 단계에서는 SVM learning에 의하여 classification을 위한 decision model을 생성하고, 여기에 테스트를 시행하여 correct rate에 의해 classification의 성능을 분석한다.

표 1은 window size가 16, sliding size가 8, pattern feature size가 9일 때 트레이닝을 하여 decision model을 생성하고, test를 시행하였을 때 실험 결과를 나타낸 것이다. Normal case 5에서 Normal(+1)을 Abnormal(-1)로 잘못 인식되어 false positive error를 발생하였고, false negative error는 발생하지 않아 90%의 correct rate를 보임을 알 수 있다.

State	$\vec{w}\cdot\vec{x}+b$	D(x)	Correctness	Total correct rate
Normal1	0.54412	+1	CORRECT	
Normal2	0.26612	+1	CORRECT	
Normal3	0.54412	+1	CORRECT	
Normal4	0.33888	+1	CORRECT	
Normal5	**-1.4985**	**-1**	**ERROR (false positive)**	**90%**
Abnormal1	-0.42349	-1	CORRECT	
Abnormal2	-0.99925	-1	CORRECT	
Abnormal3	-1	-1	CORRECT	
Abnormal4	-1.0271	-1	CORRECT	
Abnormal5	-1.7125	-1	CORRECT	

표 1: window size가 16, sliding size가 8, pattern feature size가 9일 때 실험결과

이와 같이 제안한 방법에 의한 실험을 통하여, 다음과 같은 몇 가지를 생각해 볼 수 있다. 우선 90%이상의 correct rate를 보여 SVM classification을 이용한 침입 탐지의 좋은 성능을 기대할 수 있다. 또한 반복적인 실험 결과 window size와 pattern feature size는 서로 독립적이지 않은 특성을 보이므로, 실험 범위를 더 확대하여, window size에 따라 pattern feature size를 결정하면, 좀 더 성능이 좋은 classification model을 만들 수 있을 것으로 기대된다. 덧붙여서 침입을 정상으로 잘못 인식하는 false negative correctness error가 정상을 침입으로 인식하는 false positive correctness error가 훨씬

적어 치명적인 error 발생률도 낮음을 알 수 있다.

V. 결론

본 논문에서는 이진분류에 뛰어난 성능을 발휘하는 SVM을 이용하여 침입 탐지 시스템을 구현하였다. 감사자료를 system call level에서 분석하여 training set을 구성하였고, 여기에 SVM을 적용하여 decision model을 생성하였다. 이에 대한 검증을 위하여, 이미 알려진 침입 트레이스와 정상 트레이스로 구성된 test set을 적용하여 침입 탐지 여부를 판별하였다. 실험 결과 window size와 pattern feature의 수 등에 따라 차이가 있으나, 침입과 정상에 대해서 최대 탐지율이 90% 정도의 정확도를 보였다. 이로써 SVM이 호스트 기반의 침입 탐지 시스템에 적용될 수 있는 가능성을 보였다. 그러나 본 연구에서 알려진 침입에 대한 학습 데이터가 부족하여 SVM decision model이 좋은 성능을 발휘하도록 training 시키는데 한계가 있었다. 따라서, 향후 연구로는 먼저 대량의 감사자료를 수집 또는 생성하고, 다음으로 수집된 데이터들로부터 특징을 추출하는 과정에서 최대의 분류 성능을 내기 위하여 Genetic algorithm과 연동 하는 방안을 고려할 수 있을 것이다.

참고문헌

[1] S. Kumer, E. H. Spafford, "A pattern matching model for misuse intrusion detection", In Proceedings of the 17th National Computer Security Conference, October 1994

[2] S. Kumer, E. H. Spafford, "An Application of Pattern Matching in Intrusion Detection", Technical Report CSD-TR-94-013, Purdue University, 1994

[3] J. Ryan, M. J. Lin, R. Miikkulaine, "Intrusion Detection with Neural Networks", Advanced in Neural Information Processing Systems 10, Cmbridge, MA, 1998

[4] Vladimir V.N. "The Nature of Statistical Learning Theory", Springer, Berlin Heidelberg New York, 1995

[5] S. Mukkamala, G. Janoski, A. Sung, "Intrusion Detection Using Neural Networks and Support Vector Machines" IEEE IJCNN, May, 2002

[6] S. Forrest, A. S. Perelson, L. Allen, R Cherukuri, "Self-Nonself discrimination in Computer", In Proceedings of 1994 IEEE Symposium on Computer Security and Privacy, 1996

[7] S. Forrest, S. A. Hofmeyr, A. Somayaji, and T. A. Longstaff, "A sense of self for Unix processes", In Proceedings of 1996 IEEE Symposium on Computer Security and Privacy, Los Alamitos, CA, 1996

[8] S. A. Hofmeyr, A. Somayaji, and S. Forrest, "Intrusion Detection using Sequence of System Calls", in the Journal of Computer Security, Vol. 6, 1998

[9] W. Lee, S. J. Stolfo, "Data mining approaches for intrusion detection", In Proceedings fo the Seventh USENIX Security Symposium, San Antonio, TX, 1998

[10] http://www.cs.unm.edu/~immsec/data/

[11] ftp://info.sert.org/pub/sert_advisories/