SVM을 통한 미확인 침입탐지 시스템 개발*

김석태** · 한인규** · 이창용** · 고정호**
이도원** · 오정민** · 방철수** · 이 극**

요 약

본 연구는 수집된 training 패킷을 패킷이미지 생성모듈을 통해 적절히 가공하여 SVM에 학습을 시키고 학습된 SVM에 testing 패킷이미지를 테스트 시킨 후 분류해내는 것을 제안한다. 서포트 벡터 머신[Support Vector Machines]을 이용한 미확인 침입탐지 시스템은 보안의 안정성 및 효율성면에서 기존의 시스템들보다 훨씬 우수하다.

A Development of Unknown Intrusion Detection System with SVM

Seok-Tae Kim** · In-Gyu Han** · Chang-Yong Lee** · Jeong-Ho Kho**
Do-Won Lee** · Jeong-Min Oh** · Cheol-Soo Bang** · Geuk Lee**

ABSTRACT

In this research, we suggest the unknown intrusion detection system with SVM(Support Vector Machines). At the system, at first, collected training-packets are processed through packet image creating module. And then, it is studied by the SVM module. Finally, the studied SVM module classifies the test-data unsing test-packet-image. This system's stability and efficient characteristic of security is far superior than the existing it.

Key words : SVM(Support Vector Machines, Intrusion Detection System

* 본 연구는 산업자원부 지역혁신센터사업인 민군겸용보안공학연구센터 및 bk21사업 및 한남대학교 교비학술연구지원으로 수행되었음.
** 한남대학교 컴퓨터공학과

1. 서 론

정보화가 빠른 속도로 진행되어 정보통신망에 대한 의존도가 높아지고 있고, 그에 따른 사이버테러 역시 급증하고 있다. 특히 네트워크를 통한 실시간 침입 시도 및 악성 트래픽은 시스템에 치명적인 손실을 초래할 수 있으며, 이에 대한 대응책이 시급한 상황이다. 또한 미확인 침입탐지를 위해 지속적인 네트워크의 모니터링과 분석이 요구되고 있다. 현재 침입을 예측하여 신속한 대처를 하기위해 많은 연구가 이루어지고 있으며, 미확인 침입에 대한 탐지 기술이 이유가 되고 있다.

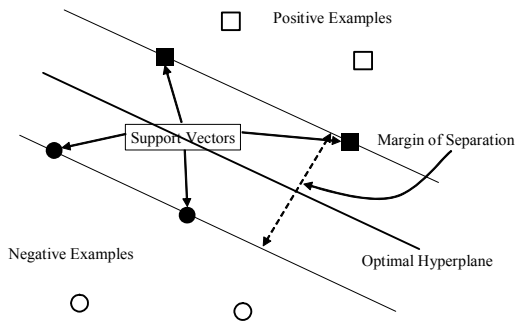
정보화 사회에서 시스템의 자원과 데이터는 국가의 중요한 자산이 되고 있다. 이에 상응하여 전쟁 또한 사이버전 또는 사이버테러의 형태로 변화하면서 국가간에 기술의 우의를 차지하기 위해 연구에 박차를 가하고 있는 실정이다. 사이버 전쟁은 신속한 공격을 통해 시스템을 마비시키고 정보를 획득하는데 목적이 있는 만큼 공격을 사전에 탐지할 수 있는 미확인 침입탐지 시스템이 요구된다. 따라서 본 논문에서는 미확인 침입으로부터 패킷분석을 통해 시스템을 안전하게 보호 할 수 있는 시스템을 제안한다.

제 2장에서는 미확인 침입탐지 시스템에 대한 관련자료들을 수집하고 분석한다. 제 3장에서는 미확인 침입탐지 시스템을 설계한다. 제 4장에서는 미확인 침입탐지 시스템을 구현하며 마지막 제 5장에서는 결론을 맺는다.

2. 관련 연구

다중클래스 침입 분류는 주어진 여러개의 침입유형별로 선별해 주는 문제이다. 침입분류 문제의 특징은 침입이 매우 높은 차원으로 표현된다는 것인데 SVM 알고리즘은 차원을 전혀 줄이지 않고 문제를 해결할 수 있다는 장점이 있다. 따라서 SVM 학습 알고리즘을 이용하여 침입 분류 문제를 다루어 미확인 위협을 예측할 수 있다.

SVM(Support Vector Machines)은 Vladimir Vapnik에 의해 고안되었다. 처음의 SVM은 선형분리 가능한 두 클래스를 구분 지으며 마진을 최대로 하는 초평면 $w \cdot x + b = 0$을 찾는 문제였다.



(그림 1) 선형 SVM

통계적 학습 이론에서, Vapnik과 Chervonenks는 모델의 복잡도의 측정 수단인 VC 차원을 도입했다. 이들은 학습 모델의 수렴 경계 조건을 다음의 식으로 제시했다.

$$R(w) \le R_{emp}(w) + \sqrt{\frac{h\left(\ln\frac{2l}{h}+1\right)-\ln\frac{\eta}{4}}{l}}, \ \forall w \in W$$

where

$$R(w) = \int |d - F(x,w)| dF_{x,D}(x, d)$$

$$R_{emp}(w) = \frac{1}{l}\sum_{i=1}^{l}|d_i - F(x_i, w)|$$

(그림 2) 학습모델의 수렴 경계 조건

여기에는 h는 VC 차원이고, 1은 학습 데이터의 수이며, R(w)는 기대 리스크(expected risk)이고 Remp(w)는 경험적 리스크(empirical risk)이다. 수렴 경계 조건이 뜻하는 바는 최적의 모델을 찾기 위해서 Remp(w)만을 최소로 하는 모델을 찾는 것만으로는 부족하고 모델 복잡도 까지 고려해야 한

다는 것이다.

그런데 대부분의 학습 기법에서 VC 차원의 측정은 어렵다. 그러나 SVM에서는 다음의 정리에 의해 VC차원의 직접적인 제어가 가능하다.

즉, 선형분리 가능 문제의 경우 Remp(w)는 항상 0이 되게 할 수 있으므로 VC 차원이 최소인 모델을 찾으면 최적의 R(w)를 찾게 된다. SVM에서 이것은 마진을 최대로 하는 즉, $||w||^2$을 최소로 하는 모델을 찾는 것으로 귀결된다.

$$\min_{w,b} \frac{1}{2}\|w\|^2 \text{ subject to } d_i(w \cdot x_i - b) \geq 1, \forall i$$

(그림 3) VC차원의 직접적인 제어를 위한 정리

선형 분리 가능이라는 제약 조건은 Cortes와 Vapnik에 해결되었다. 그들은 슬랙 변수(slack variable)를 두어 에러를 허용하고 C 파라미터를 두어 마진과 에러의 트레이드오프를 조절했다.

$$\min_{w,b,\xi} \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{l}\xi_i \text{ subject to } d_i(w \cdot x_i + b) \geq 1 - \xi_i, \forall i$$

(그림 4) 선형분리를 위한 정리

이를 라그랑쥐 듀얼 문제로 변환하면 (그림 5)와 같다.

$$\min_{\lambda} \frac{1}{2}\sum_{i=1}^{l}\sum_{j=1}^{l} d_i d_j K(x_i, x_j)\lambda_i\lambda_j - \sum_{i=1}^{l}\lambda_i$$

$$\text{subject to}$$

$$0 \leq \lambda_i \leq C, \forall i$$

$$\sum_{i=1}^{l} d_i\lambda_i = 0$$

(그림 5) 라그랑쥐 듀얼 문제로의 변환식

여기에서 K(Xi, Xj)는 커널 함수로서 비선형 함수에까지 일반화한 것이다. 이 최적화 문제의 해로 얻어지는 $0 < \lambda i < C$에 해당하는 데이터가 마진 상에 존재하는 데이터이고 이 데이터를 SV(Support Vector)라고 한다. 초평면의식은 SV만을 이용하여 (그림 6)과 같다.

$$\sum_{i=1}^{l_d} d_i\lambda_i K(x, x_i) + b = 0$$

(그림 6) 초평면의 식

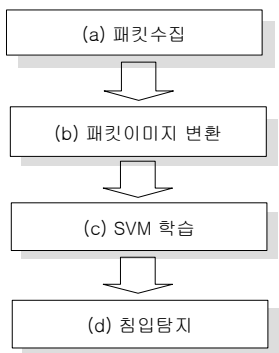
이 때 ls는 SV의 개수이다.

결국 SVM은 QP(Quadratic Programming)으로 정형화가 된다. 일반적인 QP 라이브러리는 SVM에 적용이 용이하지가 않다. SVM 학습을 위한 효과적인 QP 휴리스틱으로, Chunking, Decomposition, SMO(Sequential Minimal Optimization) 기법 등이 연구되었다.

3. 미확인 침입탐지 시스템 설계

3.1 침입탐지 시스템의 전체구성

SVM을 이용한 공격 탐지 모듈은 아래 그림과 같다. 패킷수집기는 libpcap 라이브러리를 이용하여 패킷을 수집하고, 시간, 길이, 로우(raw) 데이터를 가지는 패킷 구조체를 반환한다. 그 반환된 패킷을 가지고 패킷이미지를 생성한다. 생성된 패킷이미지를 정규화하고 SVM학습을 위해 사용된다.

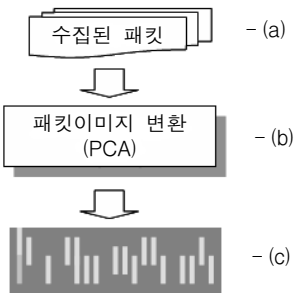


(그림 7) 침입탐지 시스템의 구성

학습이 완료되면 서포트 벡터(Support Vector, 이하 SV)가 생성된다. 생성된 SV로 실시간 네트워크 침입탐지를 하게 되고, 그 결과 정상과 비정상으로 구별하며 패킷을 연속한 패킷이미지 패턴으로 처리함으로써 공격이미지 일부분만 감지하더라도 이와 가장 유사한 패턴으로 구별하게 된다.

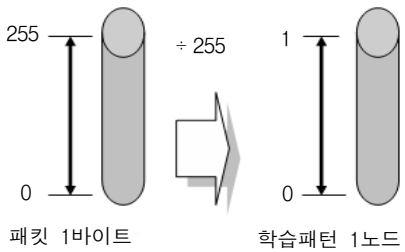
3.2 패킷 패턴 변환 및 학습 패턴 생성

수집된 패킷은 패킷이미지로 만들어 지게 된다. 만들어진 패킷이미지는 (그림 8)의(c)와 같은 spectrogram을 생성하게 된다. 세로줄은 하나의 패킷을 설명하는 주성분들을 나타내고 그것을 순차적으로 60개(Time Step) 하나의 이미지로 만들게 된다.



(그림 8) 수집된 패킷의 학습 패턴 변환

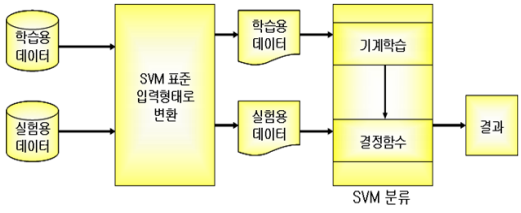
SYN Floodung, Land, TearDrop과 같은 공격들은 패킷의 60바이트 이내의 헤더정보에서 식별이 가능하다. 이러한 공격들을 구분하기 위해 패킷 60개가 하나의 이미지를 나타내도록 한다. 패킷은 1비트 단위로써 0과 1로 이루어진 바이너리 이미지이지만 1바이트를 이미지의 한 픽셀로 나타내면 그레이 이미지가 된다. 그림 9는 패킷의 그레이 이미지로써 세로줄은 하나의 패킷을 나타내고 오른쪽으로 순차적으로 60개의 패킷이 나열되게 된다. 이러한 패킷이미지를 만들어 SVM의 학습을 위해 1바이트를 1비트의 0과 1사이 값으로 바꾸기 위해 255로 나누어 나누어진 수로 그레이이미지를 만들게 된다.



(그림 9) 패킷의 학습패턴 이미지 변환

3.3 미확인 침입탐지의 개요도

(그림 10)은 SVM을 이용한 미확인 침입탐지 시스템의 개요도이며, 수집된 정보 중에서 필요한 특성 정보만을 선택하여 학습용 데이터 집합과 실험용 데이터 집합을 만든다. 이 집합들은 SVM 학습 기계의 표준 입력 폼에 합당하도록 변환되어진다. SVM은 학습용 데이터 집합을 사용하여 학습되어지고 그 결과로써 결과함수가 생성된다. 실제로 이 결정함수는 고차원 공간에서 결정평면이다. SVM의 학습은 학습용 데이터 집합과 학습에 사용되는 내부 커널함수, 또한 조정 파라미터인 C값에 의존한다. SVM의 커널함수는 고차원의 비선형의 입력값을 선형으로 변환 시켜줌으로써 SVM의 연산속도를 높이는 역할을 한다.



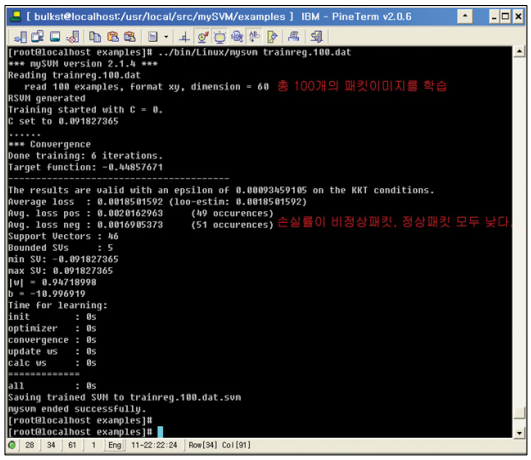
(그림 10) 미확인 침입탐지의 개요도

4. 구 현

PCA와 SVM을 이용한 침입탐지 시스템은 펜티엄 4 PC, Fedora core 4환경에서 테스트되었다.

SVM을 학습하기 위해 TearDrop 공격에 대한 정상패킷 50개 비정상 패킷 50개를 수집하여 무작위로 섞고 50개의 정상패킷과 50개의 비정상 패킷으로 만들어 학습을 하게하였다.

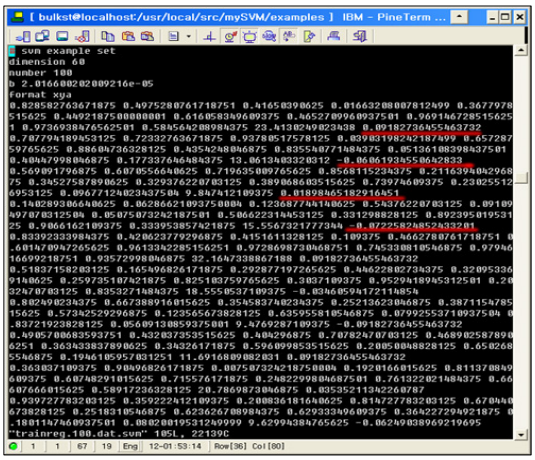
(그림 11)은 SVM의 학습결과 이며 학습에 사용한 데이터의 개수는 100개를 읽었고 6번의 학습을 반복하였다. 이 결과 패킷 분류 손실률이 0.2% 정도로 상당히 낮았고 Support vector로 46개의 패킷이미지가 선정되었다. 선정되지 못한 패킷이미지들은 마진값 안쪽에 있는 값들로 SV로써 적절치 못한 값들이다. Bounded SVs는 5로 마진 값 경계에 가장 근접한 값이다.



(그림 11) 미확인 침입탐지시스템의 학습결과

(그림 12)는 이진분류된 패킷 이미지를 보여주는 것으로 Positive (+1)은 비정상 패킷을 나타내고 Negative(-1)은 정상 패킷을 보여준다. '0'으로 분류된 경우 SV로 선택되지 못한 패킷이다.

<표 1>은 SVM 실험결과표를 나타낸다. 비정상을 정상으로 탐지한 것을 False Positive이라하고 정상을 비정상으로 탐지한 것을 False Negative라고 한다. 테스트 한것중 New TearDrop에 대해 2건의 False Negative가 검출되어 96%의 높은 검출률을 보이고 있다.



(그림 12) 이진분류된 패킷이미지

〈표 1〉 SVM 실험 결과표

	SVM	
	False Positive	False Negative
변종공격테스트	0	2

5. 결 론

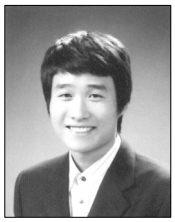
본 논문에서는 SVM을 통한 미확인 침입탐지 시스템을 구현하였다. 이 연구는 급변하는 사이버 테러의 위협에 신속히 대처하는데 유용하게 사용될 것이다.

참 고 문 헌

[1] 권윤주, "Design of the Detection and Response System against DDoS attacks", Supercomputing Center KISTI.

[2] N. Slonim and N. Tishby, "Document clustering using word clusters via the information bottleneck method", In Proceedings of SIGIR-2000, pp. 208-215, 2000.

[3] C. Certes and V. Vapnik, Support Vector Networks, Manchine Learning, Vol. 20, pp. 273-297, 1995.
[4] John C. Platt, Sequential Minimal Optimization : A Fast Algorithm for Training Support Vector Machines, Technical Report MSR-TR-98-14, 1998.
[5] Stephen G. Nash and Areila Sofer, Linear and Nonlinear Programming. McGraw-Hill, 1997.
[6] Thorsten Joachims, Making Large-Scale Support Vector Machine Learning Practical, Advances in Kernel Methods. MIT press, pp. 169-184, 1999.



김 석 태
2006년 한남대학교 컴퓨터 공학과(공학사)
2007년～현재 한남대학교 컴퓨터공학과 석사과정

한 인 규
2006년 한남대학교 컴퓨터 공학과(공학사)
2007년～현재 한남대학교 컴퓨터공학과 석사과정

이 창 용
2007년 한남대학교 컴퓨터 공학과(공학사)
2007년～현재 한남대학교 컴퓨터공학과 석사과정

고 정 호
2007년 한남대학교 컴퓨터 공학과(공학사)
2007년～현재 한남대학교 컴퓨터공학과 석사과정

이 도 원
2004년 원광대학교 컴퓨터 공학과(공학학사)
2007년 원광대학교 컴퓨터 공학과(공학석사)
2007년～현재 한남대학교 컴퓨터공학과 박사과정

오 정 민
2007년～현재 한남대학교 컴퓨터공학과 박사과정

방 철 수
2001년 연세대학교 전산정보 전공(이학석사)
2007년～현재 한남대학교 컴퓨터공학과 박사과정

이 극
1983년 경북대학교 전자과 컴퓨터공학전공(공학사)
1986년 서울대학교 컴퓨터 공학과(공학석사)
1993년 서울대학교 컴퓨터 공학과(공학박사)
1988년～현재 민군겸용 보안공학 연구센터 소장