Journal of the Korea Academia-Industrial cooperation Society
Vol. 17, No. 2 pp. 703-711, 2016

http://dx.doi.org/10.5762/KAIS.2016.17.2.703
ISSN 1975-4701 / eISSN 2288-4688

SVM과 인공 신경망을 이용한 침입탐지 효과 비교 연구

조성래[1], 성행남[2], 안병혁[1*]
[1]경상대학교 경영대학 경영정보학과, [2]경상대학교 경영대학

A Comparative Study on the Performance of SVM and an Artificial Neural Network in Intrusion Detection

Seongrae Jo[1], Haengnam Sung[2], Byung-Hyuk Ahn[1*]
[1]Dept. of MIS, College of Business, Gyeongsang National University
[2]College of Business, Gyeongsang National University

요 약 침입탐지시스템은 네트워크 데이터 분석을 통해 네트워크 침입을 탐지하는 역할을 수행하고 침입탐지를 위해 높은 수치의 정확도와 탐지율, 그리고 낮은 수치의 오경보율이 요구된다. 또한 네트워크 데이터 분석을 위해서는 전문가 시스템, 데이터 마이닝, 상태전이 분석(state transition analysis) 등 다양한 기법이 이용된다.
본 연구의 목적은 데이터 마이닝을 이용한 네트워크 침입탐지기법인 두 기법의 탐지효과를 비교하는데 있다. 첫번째 기법은 기계학습 알고리즘인 SVM이고 두번째 알고리즘은 인공 신경망 모형 중의 하나인 FANN이다. 두 기법의 탐지효과를 비교하기 위해 침입 탐지에 많이 쓰이는 KDD Cup 99 훈련 및 테스트 데이터를 이용하여 탐지의 정확도, 탐지율, 오경보율을 계산하고 비교하였다. 정상적인 데이터를 침입으로 간주하는 오경보율의 경우 SVM보다 FANN이 약간 많은 오경보율을 보이나, 탐지의 정확도 및 침입을 찾아내는 탐지율에서 FANN은 SVM보다 월등한 탐지효과를 보여준다. 정상적인 데이터를 침입으로 간주했을 때의 위험보다는 실제 침입을 정상적인 데이터로 인식할 때의 위험도가 훨씬 큰 것을 감안하면 FANN이 SVM보다 침입탐지에 훨씬 효과적임을 보이고 있다.

Abstract IDS (Intrusion Detection System) is used to detect network attacks through network data analysis. The system requires a high accuracy and detection rate, and low false alarm rate. In addition, the system uses a range of techniques, such as expert system, data mining, and state transition analysis to analyze the network data.
The purpose of this study was to compare the performance of two data mining methods for detecting network attacks. They are Support Vector Machine (SVM) and a neural network called Forward Additive Neural Network (FANN). The well-known KDD Cup 99 training and test data set were used to compare the performance of the two algorithms. The accuracy, detection rate, and false alarm rate were calculated. The FANN showed a slightly higher false alarm rate than the SVM, but showed a much higher accuracy and detection rate than the SVM. Considering that treating a real attack as a normal message is much riskier than treating a normal message as an attack, it is concluded that the FANN is more effective in intrusion detection than the SVM.

Keywords : Data Mining, Forward Additive Neural Network, IDS(Intrusion Detection System), Intrusion Detection, Neural Network, SVM(Support Vector Machine)

1. 서론

최근 사물인터넷과 다양한 웨어러블 기기들이 등장하면서 인터넷 기술은 우리의 삶에 다양한 부분에 긍정적인 영향을 주고 있으며, 보다 편리하게 정보를 얻고 업무를 수행하는데 기여하고 있다. 하지만 인터넷 기술이 다

*Corresponding Author : Byung-Hyuk Ahn(Gyeongsang National Univ.)
Tel: +82-55-772-1532 email: bahn@gnu.ac.kr
Received November 26, 2015 Revised (1st January 7, 2016, 2nd January 28, 2016)
Accepted February 4, 2016 Published February 29, 2016

양한 부분에 이용되면서 개인정보 획득, 사기, 위조, 사이버 테러 등 부당한 이익을 취하기 위한 목적으로 네트워크 침입이 시도되고 있다. 시간이 지남에 따라 공격수법이 지능화되는 추세를 보이고 있어 이에 대응하기 위한 다양한 방법을 모색하고 있다[1]. 네트워크 침입의 대표적인 사례로는 네이트의 개인정보유출, 소니 플레이스테이션 홈페이지 해킹 등의 사례를 들 수 있다.

침입은 컴퓨터의 시스템이나 네트워크의 기밀성, 무결성, 가용성을 해치거나 보안을 우회하여 접근하려는 시도를 의미한다. 침입을 대응하기 위한 방법에는 방화벽과 침입탐지시스템 등이 있으며, 방화벽은 침입으로 의심되는 패킷을 차단하는 역할을 하지만 모든 침입을 차단할 수 없기 때문에 침입탐지시스템의 역할이 요구된다. 침입탐지는 시스템과 네트워크에서 발생하는 이벤트를 모니터링하고 침입 흔적을 분석하는 과정을 의미한다. 또한 침입탐지시스템은 침입을 관리자에게 알리고 적정한 대응을 하는 역할을 수행한다[2].

최근 연구에서는 다양한 통신환경에서의 효율적인 침입탐지를 위해 다양한 모형 및 시스템을 제안하고 있으며, 다양한 데이터 마이닝 기법을 적용한 침입탐지시스템을 제안하고 있다[3-7].

본 연구는 데이터 마이닝 기법인 SVM(Support Vector Machine)과 인공 신경망의 하나인 FANN(Forward Additive Neural Network)을 이용하여 침입탐지에 대한 효과를 비교하는데 그 목적이 있다. SVM은 최근 다양한 분야에서 이용되고 있는 기계학습 알고리즘으로 우수한 성능을 보이는 것으로 알려져 있으며, FANN 기법은 역전파 알고리즘의 단점을 보완한 인공 신경망 기법으로 기존 침입탐지 연구에 적용된 적이 없는 기법이다. 본 연구에서는 DARPA(Defense Advanced Research Projects Agency)에서 개발된 KDD Cup 99 데이터세트를 이용하고 침입탐지 과정의 정확도, 탐지율, 오경보율[8]을 계산하여 그 효과를 비교하였다.

2. 이론적 배경 및 관련연구

2.1 침입탐지시스템의 정의와 분류

침입탐지시스템(IDS : Intrusion Detection System)은 데이터 전처리, 분석, 대응, 개선의 4 단계를 거쳐 네트워크, 데이터베이스 등을 포함한 시스템에서 발생하는 이벤트를 모니터링(monitoring)하여 침입을 분석하고 탐지하여 이에 대응하는 소프트웨어나 하드웨어로 구성되는 자동화 시스템이다[2,9-10]. 데이터 전처리 단계에서는 침입탐지시스템 센서로 부터 네트워크 활동에 관한 데이터를 수집하고 데이터를 분석 가능한 형태로 가공한다. 분석 단계에서는 정해진 패턴 및 규칙과 데이터를 비교하여 침입을 탐지하며, 특정 데이터가 침입으로 분류되는 경우 대응 단계로 넘어가 시스템 관리자에게 경보를 통해 침입을 알리게 된다. 개선 단계는 수집된 정보와 침입 데이터를 추후 침입탐지에 이용할 수 있도록 반영한다. 위 과정을 통해 지속적으로 보안을 강화하고 오경보율을 낮추게 되며, 또한 관리자가 시스템 정책을 만드는데 도움을 준다[11].

침입탐지시스템은 Table 1에서와 같이 크게 데이터 소스, 분석기법, 경과 시간, 제어 전략 및 대응 옵션의 5가지 기준으로 분류된다[1].

Table 1. Classification of Intrusion Detection Systems

Category	Item
Data Sources	host based
	network based
	application based
Analysis Technique	misuse based
	anomaly based
Elapsed time	real-time
	interval-based
Control Strategy	centralized
	partially distributed
	fully distributed
Response Options	active
	passive

최근에는 데이터 소스와 분석기법에 대한 연구가 많이 진행되고 있다. 데이터 소스에 의한 분류는 호스트의 시스템에서 수집된 데이터를 분석하는 호스트 기반 침입탐지시스템과 다수의 호스트에 대한 네트워크 트래픽을 분석하는 네트워크 기반 침입탐지시스템으로 구분된다. 분석기법에 의한 분류에는 이미 알려진 공격의 서명 등을 대상으로 분석하는 오용탐지와 이용자의 일반적인 행동을 바탕으로 침입을 탐지하는 비정상 행위 탐지가 있다.

2.2 연구동향

Anderson에 의해 처음 소개된 침입탐지의 개념은 Denning에 의해 침입탐지 모형으로 제시되었다[12].

Denning의 모형은 감사 데이터를 바탕으로 규칙을 생성하여 비정상 행위를 탐지하는 전문가 시스템의 형태로 구성되었다. 현재 침입탐지 분야의 탐지 기법에 대한 연구는 위 두 가지 연구를 바탕으로 진행되고 있다.

1998년 이후 DARPA에 의해 침입탐지시스템의 평가에 관한 연구가 진행되었고 연구 과정에서 시뮬레이션을 통해 공격과 정상으로 구분되는 네트워크 데이터를 추출하였으며, 이 데이터의 다른 버전인 KDD Cup 99 데이터세트는 최근의 침입탐지 연구에 많이 이용되고 있다.

Nguyen과 Choi는 KDD Cup 99 데이터세트를 이용하여 BayesNet, NaïveBayes, J48(C4.5), NBTree, Decision Table, JRip, OneR, MLP, SMO와 LBK 분류기를 이용하여 실험을 진행하여 공격유형별 정확도와 훈련시간을 비교하였다[13].

Wu와 Yen은 KDD Cup 99 데이터세트에 의사결정트리 기법인 C4.5와 기계학습 알고리즘인 SVM을 적용하여 두 기법 간 탐지의 정확도, 탐지율과 오경보율을 비교하여 C4.5는 대부분의 테스트에서 SVM보다 높은 정확도와 탐지율을 나타내었고 오경보율은 SVM에서 더 높게 나타나는 것으로 실험 결과를 제시하였다[8].

C4.5, SVM, 신경망 알고리즘을 적용하여 진행된 연구에서는 정확성 검증을 위해 훈련 데이터세트를 정상 데이터 비율에 따라 구성하고 cross-validation 기법으로 검증하였다[14-15]. 실험에서 C4.5 기법이 탐지율을 가장 높게 나타내었고 정상 데이터 비율의 증가에 따라 탐지율이 높아지는 추세를 보였다고 설명하였다.

Ibrahim 등은 침입탐지 과정을 단계 모형(phase-model)과 수준 모형(level-model)으로 분류하였다. 분류의 기법으로는 의사결정트리 기법의 알고리즘은 C5, CRT, CHAID, Quest를 이용하였다. 이 연구에서는 C5 알고리즘과 단계 모형을 적용할 경우 높은 탐지율을 나타내는 것으로 결과를 제시하였다[16].

2.3 SVM

SVM(Support Vector Machine)은 Vapnik에 의해 개발된 기계학습 알고리즘으로 지도 학습(supervised learning)에 이용된다[17]. 기본적으로 두 개의 클래스를 분류하는 문제를 다루는 기법이고 이를 확장하여 세 개 이상의 클래스를 분류하는데 이용할 수 있다. 최근 SVM은 다양한 분야에서 널리 이용되고 있으며, 우수한 성능을 보이는 것으로 알려져 있다.

2.3.1 선형 SVM

N개의 데이터를 포함하는 훈련 표본이 있고 각 데이터는 p개의 속성을 가지며, 두 개의 클래스에 포함된다고 가정한다. 훈련 집합의 두 클래스가 선형으로 분리 가능한 경우라면 훈련 집합의 각 데이터는 p차원의 공간에서 Fig. 1의 (a)와 같이 나타낼 수 있으며, 이는 하이퍼플레인(hyperplane)으로 분리할 수 있다. SVM은 두 개의 클래스를 분류할 수 있는 최적의 하이퍼플레인을 찾는 문제를 다룬다.

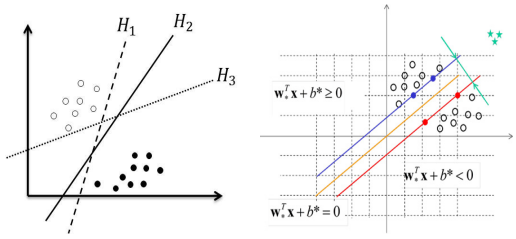

Fig. 1. Linear SVM
(a) Hyperplane (b) Support Vector

두 개의 클래스에 대한 하이퍼플레인은 아래식과 같이 표현할 수 있다.

$$\mathrm{w}_*^T\mathrm{x}+b^*\geq 0 \quad \text{for } d_i=+1$$
$$\mathrm{w}_*^T\mathrm{x}+b^*<0 \quad \text{for } d_i=-1$$

분리성의 가정에 따라 분리 하이퍼플레인과 두 클래스에 속하는 점들 중 최적의 하이퍼플레인과 가장 근접한 점의 거리가 1이 되도록 가중치를 수정할 수 있으며, 이 때 그 근접한 점들을 서포트 벡터(support vector)라고 하며 Fig. 1의 (b)와 같이 표현할 수 있다.

두 개의 클래스에 대한 각각의 하이퍼플레인 식에 서포트 벡터를 대입하면 두 개의 서포트 벡터의 거리를 최대로 하는 분리 하이퍼플레인을 찾는 문제로 접근할 수 있고 이 문제는 아래와 같이 최적화 문제로 접근할 수 있다.

$$\min.\ \Phi(\mathrm{w})=\frac{1}{2}\mathrm{w}^{\mathrm{T}}\mathrm{w}$$
$$s.t.\ \ d_i(\mathrm{w}^{\mathrm{T}}\mathrm{x}_{\mathrm{i}}+b)\geq 1 \ \text{ for } i=1,2,\ldots,N$$

2.3.2 비선형 SVM

Fig. 2와 같이 두 클래스를 선형으로 분류하기 어려운 경우 비선형 SVM으로 분류할 수 있다. 비선형 SVM에서는 선형 SVM으로 분리가 불가능한 훈련 데이터에 대해 커널 기법(kernel method)를 이용한다. 커널 기법이란 입력 데이터를 어떤 특성으로 조직화하고 이를 고차원의 특성 공간(feature space)에 매핑(mapping)하는 기법이다. 커널 함수(kernel function)는 입력 데이터를 특성 공간에 매핑하는 역할을 수행하며, 대개 두 개의 데이터를 하나의 특성으로 조직화한다. 커널함수는 아래 식과 같다.

$$k(\mathrm{x}, \mathrm{x}_i) = \varphi^T(\mathrm{x}_i)\varphi(\mathrm{x}) = \sum_{j-1}^{\infty}\varphi_j(\mathrm{x}_i)\varphi_j(\mathrm{x}), \quad i = 1,2,...,N_s$$

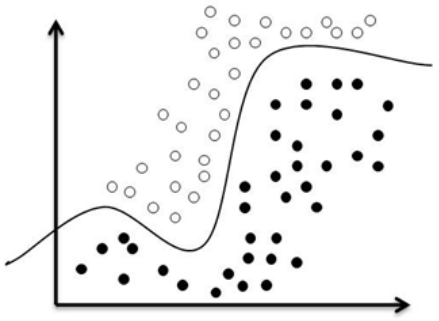

Fig. 2. In Case of Non-linear Separation

두 개의 클래스에 대한 하이퍼플레인은 아래식과 같이 표현할 수 있다.

2.4 인공 신경망

인공 신경망은 노드(node)와 아크(arc)로 구성되며, 인공 신경망의 네트워크 구조는 노드의 수와 각 노드의 연결을 포함한다. 활성화 함수는 입력을 출력으로 변형하는 역할을 하고 훈련 규칙은 각 아크의 가중치(weight)를 결정한다. 지도 학습(supervised learning)은 패턴에 대해 목표로 설정된 클래스를 레이블의 형태로 포함하고 자율 학습(unsupervised learning)은 레이블이 없는 훈련 데이터를 이용한다.

최초의 신경망 모형은 McCulloch와 Pitt에 의해 개발되었고, Rosenblatt는 단층 퍼셉트론(single-layer perceptron)을 제안하였다[18-19]. Minsky와 Papert가 다층 퍼셉트론(multi-layer perceptron)을 제안하고, Rumelhart 등이 다층 퍼셉트론의 학습 알고리즘인 델타룰을 소개한 이후 신경망 모형에 대해 폭넓은 연구가 진행되었다[20-21].

Feedforward 네트워크는 네트워트 상의 정보가 한 방향으로만 전송되는 네트워크로 대표적인 훈련 방법은 역전파 알고리즘(back propagation algorithm)이며, 역전파 알고리즘은 최급하강법(steepest descent method)의 특별한 형태로 볼 수 있다. 최급하강법은 점진적인 이동의 반복을 통해 해에 접근하기 때문에 수행 속도가 느린 단점이 있다. 또한 역전파 알고리즘이나 gradient 기반 알고리즘들은 지역 최소치(local minima)에 수렴하는 경우가 있어 네트워크의 훈련에 어려움이 주기도 한다. Fig. 3 은 3계층 feedforward 네트워크의 나타낸다.

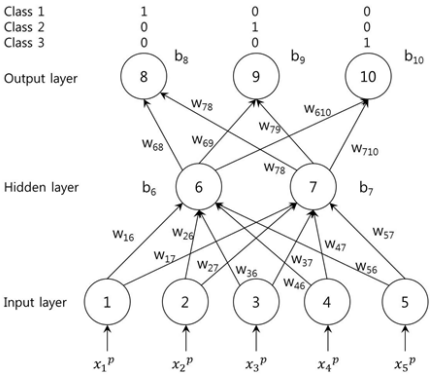

Fig. 3. 3-layer feedforward networks

본 연구에서 역전파 알고리즘의 단점을 보강한 FANN 모형을 통해 효율적인 비선형 최적화 알고리즘을 사용하며, 통계적 검증에 의해 네트워크의 크기를 최소화 하였다. FANN 모형의 특징은 다음과 같다[22].

- FANN 모형은 효율적인 지역 탐색을 위해 비선형 최소화 기법인 limited memory BFGS(Broyden – Fletcher – Goldfarb – Shanno) 기법을 이용한다.
- FANN 모형은 훈련의 성과에 큰 영향을 줄 수 있는 역전파 알고리즘의 학습률이나 momentum 같은 조정을 위한 파라미터(parameter) 값은 가지지 않는다.
- FANN 모형은 네트워크 아크의 가중치 의 최소값(initial solution)을 난수(random number)로 정하

지 않고 활성화 함수로 1차 함수를 사용함으로써 결과적으로 선형 회귀분석의 결과를 초기값으로 사용한다.

- FANN 모형은 네트워크의 은닉 노드 추가에 따른 오차제곱합(sum of squared errors)의 감소를 보장한다.
- FANN 모형은 모형의 결정을 위해 통계적 검증을 이용하여 최소한의 네트워크 크기를 결정하며, 훈련된 네트워크는 실제 문제에 적용될 때 통계적 신뢰를 가질 수 있다.

3. 연구설계 및 실험

3.1 연구과정

본 연구의 분석과정은 Fig. 4와 같다. 본 연구에서는 KDD Cup 99 데이터세트를 이용하여 연구의 목적에 맞게 샘플링하고 적절한 형태로 변형하는 데이터 전처리의 과정을 거친 후, SVM 기법의 훈련과 테스트를 위해 Weka 데이터 마이닝 도구를 이용하였으며, FANN 기법의 훈련과 테스트는 별도의 작성된 프로그램을 이용하여 연구를 진행하였다. 분석 및 결과 비교 단계에서는 두 기법의 테스트에 대한 정확도(accuracy), 탐지율(detection rate), 오경보율(false alarm rate)를 계산하여 비교하였으며, 이를 바탕으로 결론을 도출하였다.

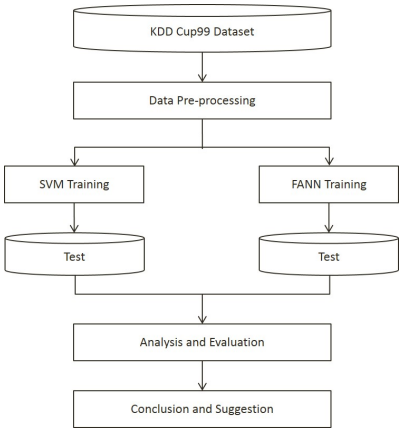

Fig. 4. Research Process

3.2 KDD Cup 99 데이터세트

본 연구에서는 KDD Cup 99 데이터세트를 이용하여 테스트 및 분석을 진행하였다. KDD Cup 99 데이터세트는 1998년 DARPA(Defense Advanced Research Projects Agency)에서 침입탐지 분야에 대한 연구를 목적으로 군사 네트워크 환경에서 시뮬레이션을 통해 얻어진 네트워크 트래픽의 TCP dump 데이터를 이용하여 1999년 KDD Cup 대회를 위해 가공된 버전이다. KDD Cup 99 데이터세트는 발표된 시점으로부터 10여년의 시간적 차이가 있고 새로운 공격유형의 등장과 네트워크 환경의 변화에도 불구하고 침입탐지 분야에서 널리 이용되는 데이터이다[6,8,16,23]. KDD Cup 99 데이터세트는 정상 데이터와 Probe, DoS, U2R, R2L의 4가지 공격유형으로 구성된다.

Probe 공격은 다른 공격을 준비하는 단계로서 네트워크상에 존재하는 IP 주소, 제공되는 서비스의 콘텐츠 또는 운영체제의 종류 등과 같은 정보를 획득하거나 특정 시스템의 취약점을 찾는데 중점을 둔다. 특히 Satan, Saint, Mscan과 같은 도구들은 숙련도가 낮은 공격자(attacker)들에게도 네트워크에 존재하는 장비들의 취약점을 신속하게 발견할 수 있도록 도와준다.

DoS(Denial of Service) 공격은 공격자가 특정 시스템 자원 전체를 점유하거나 대역폭 또는 시스템 자원에 장애를 발생시켜 정당한 사용자들의 접근을 거부하는 형태의 공격이다[16].

U2R(User to Root) 공격은 공격자가 특정 시스템에 일반 사용자 권한으로 접근한 다음 buffer-overflow와 같은 공격으로 취약점을 이용해 루트 권한을 획득하는 형태의 공격이다.

R2L(Remote to Local) 공격은 공격자가 호스트 장비의 취약점을 이용하여 인증되지 않은 접근권한을 다양한 방법으로 획득하여, 호스트 장비에 불법적으로 접근하는 공격 방법이다.

3.3 데이터 전처리

본 연구에서는 연구과정의 일반적인 컴퓨터 환경과 연구의 목적을 고려하여 대용량 데이터인 KDD Cup 99 데이터세트를 이용하기 위해 데이터 전처리 과정을 거쳐 연구를 진행하였다. 본 연구에서는 10% KDD Cup 99 데이터세트를 이용하여 훈련 표본을 추출하였으며, 테스트 표본 추출을 위해서는 Corrected 10% 테스트 데이터세트를 이용하였다. 위 데이터세트는 41개의 속성 외에 세부 공격 패턴을 포함하고 있어 연구의 두 기법의 효율

성을 평가하는데 유용하게 사용되었다. 텍스트 파일 형식인 데이터세트는 MS-Access로 데이터베이스화 하였으며, 37개의 세부 공격패턴으로 구성된 공격 데이터 속성은 연구의 목적에 맞게 Probe, DoS, U2R, R2L의 공격유형으로 변환하여 연구를 진행하였다[7]. 훈련과 테스트에 이용된 데이터세트의 용량과 레코드 수는 Table 2와 같다.

Table 2. File Size and Record of Dataset

	File Size (MB)	Record (ea)	Remark
10% KDD Cup 99	71.4	494,021	-
Corrected 10% test	45.0	311,029	Including Attack Pattern Label

훈련 표본은 10% KDD Cup 99 데이터세트를 이용하여 정상 데이터 비율을 각각 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90%로 포함하고 공격 데이터 비율을 각각 90%, 80%, 70%, 60%, 50%, 40%, 30%, 20%, 10%로 포함하도록 구성하였으며, 10% KDD Cup 99 데이터세트에서 나타나는 공격유형별 비율에 맞추어 랜덤으로 추출하였다. 테스트 표본은 Corrected 10% 테스트 데이터세트에서 나타나는 정상 데이터와 공격 데이터의 비율에 근거하여 랜덤으로 추출하였다.

각 표본 데이터는 SVM 기법의 훈련과 테스트를 위에 Weka에서 사용하는 ARFF 파일 형식과 FANN 기법의 훈련 및 테스트를 위한 MS-Access 파일 형식으로 변환하여 연구를 진행하였다.

3.4 훈련 및 테스트

본 과정에서는 전처리 된 데이터세트를 이용하여 SVM과 FANN 기법을 적용하여 훈련 및 테스트를 진행하였다. 정상 데이터의 비율에 따라 생성된 9개의 훈련 데이터세트를 사용하여 데이터 훈련을 진행하였고, 이를 바탕으로 9회에 걸쳐 테스트를 진행하였다. 이 중 SVM 기법은 Weka에 LIBSVM 라이브러리를 추가하여 연구를 진행하였다. LIBSVM은 다양한 SVM 모형을 적용할 수 있는 통합 소프트웨어로 두 클래스나 여러 클래스를 분류하기 위한 SVC(support vector classification), 회귀분석을 위한 SVR(support vector regression)과 단일 클래스 SVM의 3가지 기능을 포함하고 있다[24]. FANN 기법은 Ahn의 C++로 작성된 프로그램을 이용하였다[22].

4. 분석 및 평가

분석 및 평가 단계에서는 정상 데이터 비율이 다른 9개의 훈련 데이터를 적용하여 얻어진 SVM 기법과 FANN 기법의 침입탐지 효과를 비교하기 위해 테스트 결과의 정확도, 탐지율, 오경보율을 계산하고 비교하였다. 계산을 위해 테스트 된 각 클래스의 데이터의 수를 Table 3 과 같이 분류한다. TP(True Positive)는 실제로 공격인 데이터가 공격으로 분류되는 경우, FP(False Positive)는 실제로 정상인 데이터가 공격으로 분류되는 경우이며, 오경보(false alarm)라고도 한다. FN(False Negative)는 실제로 공격인 데이터가 정상으로 분류되는 경우, TN(True Negative)는 실제로 정상인 데이터가 정상으로 분류되는 경우를 의미한다.

Table 3. Types of Classification of Data

	Attack (Predicted)	Normal (Predicted)
Attack(Actual)	TP	FN
Normal(Actual)	FP	TN

4.1 정확도

정확도는 데이터가 올바르게 분류된 비율을 의미한다. 즉, 실제로 공격인 데이터가 공격으로 분류된 경우, 실제로 정상인 데이터가 정상으로 분류된 경우의 비율을 의미한다. 그 식은 아래와 같다.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \times 100\%$$

Table 4 는 두 기법으로 테스트한 결과로부터 얻은 정확도를 보여준다. 9번의 모든 테스트에서 FANN 기법이 월등히 높은 정확도를 나타내었다. SVM 기법의 정확도 평균은 78.25%, FANN 기법의 정확도 평균은 92.16%로 났으며, 두 기법의 정확도 평균은 13.91%의 차이를 보였다. FANN 기법은 정상 데이터 비율이 증가하여도 91%에서 93%의 범위에서 일정한 정확도를 나타내었으나, SVM 기법은 정상 데이터 증가에 따라 정확도가 낮아지는 추세를 보였다.

Table 4. Comparison of Accuracy

Normal Data Rate	SVM(%)	FANN(%)
10%	80.49	92.70
20%	79.08	92.57
30%	78.11	92.28
40%	78.46	92.31
50%	78.24	92.36
60%	77.73	92.06
70%	78.11	91.62
80%	77.49	92.16
90%	76.55	91.37
평균	78.25	92.16

4.2 탐지율

탐지율은 실제로 공격인 데이터가 정확하게 공격으로 분류된 데이터의 비율을 의미하고 그 식은 아래와 같다.

$$Detection\ Rate = \frac{TP}{TP+FN} \times 100\%$$

Table 5. Comparison of Detection Rate

Normal Data Rate	SVM(%)	FANN(%)
10%	75.79	91.23
20%	74.04	91.18
30%	72.83	90.78
40%	73.26	90.82
50%	72.99	90.80
60%	72.35	90.46
70%	72.83	89.94
80%	72.04	90.60
90%	70.88	89.59
평균	73.00	90.60

Table 5 는 두 기법으로 테스트한 결과로부터 얻은 탐지율을 보여준다. 정확도의 결과와 같이 모든 테스트에서 FANN 기법의 탐지율이 월등히 높게 나타났다. SVM 기법의 탐지율 평균은 73.00%, FANN 기법의 탐지율 평균은 90.60%로 났으며, 두 기법의 탐지율 평균은 17.60%의 차이를 보였다. 두 기법 모두 정상 데이터 비율의 증가에 따라 탐지율이 감소하는 추세를 보이고 있으나 SVM 기법의 탐지율이 더 큰 폭으로 감소하고 있음을 확인할 수 있었다.

4.3 오경보율

오경보율은 실제로 정상인 데이터가 공격으로 잘못 분류된 경우의 비율을 의미하고 그 식은 아래와 같다.

$$False\ Alarm = \frac{FP}{FP+TN} \times 100\%$$

Table 6은 두 기법으로 테스트한 결과로부터 얻은 오경보율을 보여준다. 모든 테스트에서 SVM 기법의 오경보율이 상대적으로 낮게 나타났다. SVM 기법의 오경보율 평균은 0.05%, FANN 기법의 오경보율 평균은 1.40%로 났으며, 두 기법의 오경보율율 평균은 1.35%의 차이를 보였다.

Table 6. Comparison of False Alarm Rate

Normal Data Rate	SVM(%)	FANN(%)
10%	0.10	1.23
20%	0.10	1.69
30%	0.05	1.54
40%	0.05	1.54
50%	0.05	1.18
60%	0.05	1.33
70%	0.05	1.44
80%	0.00	1.39
90%	0.00	1.28
평균	0.05	1.40

5. 결론

침입탐지시스템은 다양한 분석기법을 적용하여 높은 탐지율과 정확도를 나타내는 방향으로 연구가 진행되고 있다. 또한 침입탐지시스템은 낮은 오경보율을 나타내어야 한다. 본 연구에서는 SVM과 FANN의 두 가지 데이터 마이닝 기법을 적용하여 침입탐지 과정의 정확도, 탐지율, 오경보율을 바탕으로 기법 간 침입탐지 효율성을 측정 및 비교하였다. 훈련 및 테스트에는 침입탐지 분야에서 널리 이용되는 KDD Cup 99 데이터세트를 이용하였고 연구의 목적에 맞게 데이터 전처리, 표본 추출의 과정을 거쳐 실험 데이터를 구성하였다. 본 연구는 기존의 침입탐지 연구에 적용된 적이 없는 FANN 기법을 이용하여 실험을 진행한 점에 그 의미가 있다.

본 연구의 실험에서 FANN 기법이 정확도와 탐지율의 면에서 SVM 기법에 비해 월등히 높은 수치를 나타내었다. 탐지율은 두 기법 모두에서 정상 데이터 비율이 증가함에 따라 감소하는 추세를 보였으며, 그 폭은 SVM 기법에서 높게 나타났다. SVM 기법은 낮은 오경보율을 나타내었다. 비록 FANN 기법이 SVM보다 오경보율이 약가 높으나 그 차이는 1.35%인데 반해 정확도와 탐지율에서는 FANN기법이 각각 13.91%와 17.6% 만큼 높은 결과를 보여준다. 침입 공격을 탐지함에 있어서 정상 데이터를 공격으로 인식하는 오류의 위험보다 공격 데이터를 정상 데이터로 인식하는 오류의 위험이 훨씬 크다는 점을 감안하면 침입탐지에 있어서 FANN기법이 보다 효과적이라고 할 수 있다.

인공 신경망 모형인 FANN 기법으로 실험을 진행하는 과정에서 하나의 은닉 노드를 사용하였음에도 불구하고 높은 정확도와 탐지율을 나타내는 것은 본 연구의 문제가 선형에 가까운 문제로 판단된다.

본 연구의 실험에 의해 도출된 시사점과 향후 연구 과제는 다음과 같다.

첫째 본 연구는 FANN 기법과 기존 연구에 사용된 기법 간 탐지 효과를 비교하는데 있었다. FANN 기법은 탐지의 정확도와 탐지율에서 SVM에 비해 높은 수치를 나타내었다. 하지만 높은 수치의 오경보율을 보이는 것은 어느 정도 과적합(overfitting)이 일어난 것으로 판단된다.

둘째 본 연구는 연구 목적 및 환경을 고려하여 제한적인 수의 데이터를 이용하였다. 따라서 본 연구의 결과를 일반화하기 위해서는 실험 데이터의 전체 데이터세트를 이용하여 연구를 진행할 필요가 있고 KDD Cup 99 데이터세트 외에 현재의 공격 기법이나 네트워크 환경을 반영하는 데이터를 이용하여 연구를 진행하는 것도 중요한 의미가 있을 것이다.

셋째 본 연구에서는 각 모형을 보다 정교하게 구성하지 못한 점이 있다. 연구에서 사용된 세 모형은 모두 해당 소프트웨어에서 정한 default 값을 기초로 하였다. 따라서 보다 나은 탐지 성과를 위해 각 모형을 정교하게 작성할 필요가 있다.

넷째 본 연구에서 높은 정확도와 탐지율을 보인 기법은 높은 오경보율을 나타내었다. 현재의 침입탐지시스템은 보다 높은 정확도와 탐지율과 동시에 낮은 오경보율을 요구한다. 따라서 이 세 가지 평가 기준을 모두 만족할 수 있는 방안을 모색할 필요가 있다.

References

[1] Dea-Woo Park, “Consideration for Hacking on National Cyber Security Policy,” Review of KIISC, Vol. 21, No. 6, pp. 24-41, 2011.

[2] Bace, R. and Mell, P., NIST Special Publication on Intrusion Detection Systems, BOOZ-ALLEN AND HAMILTON INC MCLEAN VA, 2001.
DOI: http://dx.doi.org/10.6028/NIST.SP.800-31

[3] Hwan Seok Yang, “The Study on Rules for Performance Improvement of Intrusion Detection System,” The Journal of KINGComputing, Vol. 5, No. 3, pp. 43 - 49, 2009.

[4] Kyu Won Lee, Jae Won Ji, Hyun Woo Chun, Sang-jo Youk , Geuk Lee, “Traffic Analysis Technique for Intrusion Detectionin in Wireless Network,” Journal of Security Engineering, Vol. 7, No. 6, pp. 599 - 607, 2010.

[5] Abadeh, M. S., Habibi, J., and Lucas, C., “Intrusion Detection Using a Fuzzy Genetics-based Learning Algorithm,” Journal of Network and Computer Applications, Vol. 30, No. 1, pp. 414-428, 2007.
DOI: http://dx.doi.org/10.1016/j.jnca.2005.05.002

[6] Zarrabi, A. and Zarrabi, A., “Internet Intrusion Detection System Service in a Cloud,” International Journal of Computer Science Issues, Vol. 9, Issue 5, No. 2, pp. 308-315, 2012.

[7] Fares, A. H., Sharawy, M. I., and Zayed, H. H., “Intrusion Detection: Supervised Machine Learning,” Journal of Computing Science and Engineering, Vol. 5, No. 4, pp. 305-313, 2011.
DOI: http://dx.doi.org/10.5626/JCSE.2011.5.4.305

[8] Wu, S. and Yen, E., “Data Mining-based Intrusion Detectors,” Expert Systems with Applications, Vol. 36, No. 3, pp. 5605 - 5612, 2009.
DOI: http://dx.doi.org/10.1016/j.eswa.2008.06.138

[9] Beigh, B. M. and Peer, M. A., “Intrusion Detection and Prevention System: Classification and Quick Review,” ARPN Journal of Science and Technology, Vol. 2, No. 7, pp. 661 - 675, 2012.

[10] Kumar, Y. and Dhawan, S., “A Review on Information Flow in Intrusion Detection System,” International Journal of Computational Engineering and Management, Vol. 15, No. 1, pp. 91 - 96, 2012.

[11] Singaraju, S. and Kalpana, P., “A Precise Survey on Intrusion Detection Systems,” International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 9, pp. 243 - 247, 2012.

[12] Denning, D. E., “An Intrusion-Detection Model,” IEEE Transaction on Software Engineering, Vol. 13, No. 2, pp. 222 - 232, 1987.
DOI: http://dx.doi.org/10.1109/TSE.1987.232894

[13] Nguyen, H. A., and Choi. D., “Application of Data Mining to Network Intrusion Detection: Classifier Selection Model,” Challenges for Next Generation Network Operations and Service Management -Lecture Notes in Computer Science, Vol. 5297, pp. 399-408, 2008.

[14] Jalil, K. A., Kamarudin, M. H., and Masrek, M. N., “Comparison of Machine Learning Algorithms

Performance in Detecting Network Intrusion," Networking and Information Technology 2010 International Conference, pp. 221 – 226, 2010.

[15] Osareh, A. and Shadgar, B., "Intrusion Detection in Computer Networks Based on Machine Learning Algorithms," International Journal of Computer Science and Network Security, Vol. 8, No. 11, pp. 15-23, 2008.

[16] Ibrahim, H. E., Badr, S. M., and Shaheen, M. A., "Phases vs. Levels using Decision Trees for Intrusion Detection Systems," International Journal of Computer Science and Information Security, Vol. 10, No. 8, pp. 1-7, 2012.

[17] Vapnik, V. N., The Nature of Statistical Learning Theory, Springer, 1995.
DOI: http://dx.doi.org/10.1007/978-1-4757-2440-0

[18] McCulloch, Warren S., and Walter Pitts., "A logical Calculus of the Ideas Immanent in Nervous Activity," The Bulletin of Mathematical Biophysics, Vol. 5, No. 4, pp. 115-133, 1943.
DOI: http://dx.doi.org/10.1007/BF02478259

[19] Rosenblatt, F., Principle of Neuro Dynamics, Washington, D.C.:Spartan Books, 1962.

[20] Minsky, M., and Papert, S., Perceptrons, Cambridge, MA : MIT Press, 1969.

[21] Rumelhart, D. E., Hilton, G. E., and Williams, R. J., "Learning Internal Representation by Error Propagation," ICS Report, Institute for Cognitive Science, University of California, San Diego, 1986.

[22] Ahn, B. H., "Forward Additive Neural Network Models," PhD dissertation, Kent State University, Kent, OH, USA, 1996.

[23] Hansung Lee, Younghee Im, Jooyoung Park, Daihee Park, "Adaptive Intrusion Detection System Based on SVM and Clustering ," Journal of Korean Institute of Intelligent Systems, Vol. 13, No. 2, pp. 237 – 242, 2003.

[24] Chang, C. C. and Lin, C. J., "LIBSVM: A Library for Support Vector Machine," ACM Transactions on Intelligent Systems and Technology, Vol. 2, No. 3, pp. 1-27, 2011.
DOI: http://dx.doi.org/10.1145/1961189.1961199

조 성 래(Seongrae Jo) **[준회원]**

- 2010년 8월 : 경상대학교 경영대학 경영정보학과 (경영학학사)
- 2013년 2월 : 경상대학교 대학원 경영정보학과 (경영학석사)
- 2013년 7월 ~ 2015년 7월 : Tai Woo Ree Engineering

<관심분야>
데이터마이닝, 빅데이터, 인공 신경망

성 행 남(Haengnam Sung) **[정회원]**

- 2003년 2월 : 경상대학교 대학원 경영정보학과 (경영학석사)
- 2009년 2월 : 경상대학교 대학원 경영정보학과 (경영학박사)
- 2004년 3월 ~ 현재 : 경상대학교 경영대학 강사

<관심분야>
경영정보시스템, 전자상거래, e러닝

안 병 혁(Byung-Hyuk Ahn) **[정회원]**

- 1980년 2월 : 서울대학교 경영학과 (경영학석사)
- 1989년 2월 : 미시간주립대학교 경영학과 (MSinOR석사)
- 1996년 8월 : 켄트주립대학교 경영학과 (경영학박사)
- 1996년 9월 ~ 현재 : 경상대학교 경영대학 경영정보학과 조교수, 경영경제연구소 리서치 펠로우

<관심분야>
데이터베이스시스템, 데이터마이닝, 최적화모델