지능정보연구 제18권 제1호 2012년 3월(pp.125~141)

비용효율적 지능형 침입탐지시스템 구현을 위한 유전자 알고리즘 기반 통합 모형

이현욱
국민대학교 비즈니스IT전문대학원
(900757@naver.com)

김지훈
국민대학교 비즈니스IT전문대학원
(nji77@daum.net)

안현철
국민대학교 경영대학 경영정보학부
(hcahn@kookmin.ac.kr)

본 연구는 최근 그 중요성이 한층 높아지고 있는 침입탐지시스템(IDS, Intrusion Detection System)의 침입탐지모형을 개선하기 위한 방안으로 유전자 알고리즘에 기반한 새로운 통합모형을 제시한다. 본 연구의 제안모형은 서로 상호보완적 관계에 있는 이분류 모형인 로지스틱 회귀분석(LOGIT, Logistic Regression), 의사결정나무(DT, Decision Tree), 인공신경망(ANN, Artificial Neural Network), 그리고 SVM(Support Vector Machine)의 예측결과에 적절한 가중치를 부여해 최종 예측결과를 산출하도록 하였는데, 이 때 최적 가중치의 탐색을 위한 방법으로는 유전자 알고리즘을 사용한다. 아울러, 본 연구에서는 1차적으로 오탐지율을 최소화하는 최적의 모형을 산출한 뒤, 이어 비대칭 오류비용 개념을 반영해 오탐지로 인해 발생할 수 있는 전체 비용을 최소화할 수 있는 최적 임계치를 탐색, 최종적으로 가장 비용 효율적인 침입탐지모형을 도출하고자 하였다. 본 연구에서는 제안모형의 우수성을 확인하기 위해, 국내 한 공공기관의 보안 센서로부터 수집된 로그 데이터를 바탕으로 실증 분석을 수행하였다. 그 결과, 본 연구에서 제안한 유전자 알고리즘 기반 통합모형이 인공신경망이나 SVM만으로 구성된 단일모형에 비해 학습용과 검증용 데이터셋 모두에서 더 우수한 탐지율을 보임을 확인할 수 있었다. 비대칭 오류비용을 고려한 전체 비용의 관점에서도 단일모형으로 된 비교모형에 비해 본 연구의 제안모형이 더 낮은 비용을 나타냄을 확인할 수 있었다. 이렇게 실증적으로 그 효과가 검증된 본 연구의 제안 모형은 앞으로 보다 지능화된 침입탐지시스템을 개발하는데 유용하게 활용될 수 있을 것으로 기대된다.

논문접수일 : 2012년 03월 11일 게재확정일 : 2012년 03월 19일
투고유형 : 학술대회우수논문 교신저자 : 안현철

1. 서론

오늘날 컴퓨터 및 네트워크 기술이 급속도로 발전하면서 이들 기술에 대한 기업이나 조직들의 의존도 역시 급격히 높아지고 있는 가운데, 최근 네트워크에 연결된 기업이나 조직들의 정보시스템에 서비스 장애나 마비를 불러일으키고자 하는 악의적인 공격시도가 함께 급증하고 있다(한국인터넷진흥원, 2011). 그런데, 더 큰 문제는 이러한 공격의 유형이 계속 진화해 나가고 있으며, 점차 지능화, 분산화, 자동화 되어가고 있다는 점이다. 이처럼 그 위험이 점차 증대되고 있는 네트워크 공격으로부터 정보시스템을 보호하기 위한 정보보호 체계에 대한 사회적 관심과 수요가 증대되고 있는 상황에서, 그 대안으로 침입탐지시스템(Intrusion Detection System, IDS)에 대한 학계와 산업계의

* 본 논문은 2012년도 국민대학교 교내연구비를 지원받아 수행된 연구임.
본 연구는 2012년도 국민대학교 우수연구센터사업비를 지원받아 수행된 연구임.

관심이 높아지고 있다(이종혁 외, 2004).

기존의 침입탐지시스템의 패턴 분석에 사용되었던 침입탐지모형은 전문가들의 정성적 지식을 수치화된 모형으로 구성하여 네트워크의 불법 침입자 및 해커의 행위를 식별함으로써, 비정상적인 활동에 대한 접근을 제한하는 것이 일반적인 형태였다. 이러한 전문가들의 지식에 기반을 한 침입탐지모형은 알려진 네트워크 공격 패턴 또는 비정상적인 활동에 대해서는 우수한 성과를 보이지만 새로운 패턴 및 사전 등록되지 않은 패턴에 대해서는 매우 취약하다는 단점이 있다(김한성, 2003). 이에 따라 새로운 패턴에도 능동적으로 대응할 수 있는 다양한 인공지능 기법을 활용한 지능형 침입탐지모형 개발에 대한 연구가 최근까지 활발하게 이루어지고 있다(홍태호 외, 2004; 이현욱, 안현철, 2011; Joo et al., 2003; Lee and Kim, 2006 등).

기존 문헌들의 경우, 로지스틱 회귀분석(Logistic Regression, 이하 LOGIT), 의사결정나무(Decision Trees, 이하 DT), 인공신경망(Artificial Neural Network, 이하 ANN), SVM(Support Vector machine) 등 단일 기법에 주로 초점을 두어 침입탐지모형을 연구하여 왔다. 하지만, 각각의 단일기법간 상호보완적 관계에 있는 다양한 이분류 모형들(binary classification models)을 적절하게 결합할 경우, 더 나은 예측성과를 얻을 수 있다는 연구결과를 얻을 수 있었다. 특히, 주가지수 등락 예측, 중소기업의 부실이나 도산 예측과 같은 경영 전반 분야의 예측 문제에서 이러한 이분류 모형의 결합을 통해 예측이 상대적으로 더 우수한 성과가 나타난다는 실증적 분석 결과가 일부 연구에서 제시되어 왔다(김선웅 외, 2010; 안현철 외, 2009 등).

이러한 배경에서, 본 연구에서는 유전자 알고리즘(Genetic Algorithms, 이하 GA)을 기반한 다수의 이분류 모형들을 결합한 통합모형을 활용하여 지능형 침입탐지시스템을 제안하고자 한다. 본 연구의 제안모형은 1차적으로 오판률을 최소화하는 최적의 GA 결합모형을 산출한 뒤, 이어 비대칭 오류비용 개념(asymmetric costs of errors)을 반영해 오탐지로 인해 발생할 수 있는 전체 비용을 최소화할 수 있는 최적 임계치를 탐색, 최종적으로 가장 비용 효율적인 침입탐지모형을 도출하도록 설계되어 있다. 즉, 상대적으로 False-Positive Error보다 비용이 더 큰 False-Negative Error로 인한 오판률을 효과적으로 통제할 수 있도록 최적의 임계치를 반영한 최종 모형이 도출될 수 있도록 하였다.

이어 진행될 본 논문의 구성은 다음과 같다. 우선 제 2장에서는 본 연구와 관련된 이론적 배경으로서 침입탐지시스템과 비대칭 오류비용, 그리고 LOGIT, DT, ANN, 그리고 SVM을 포함한 개별 모형에 대해 간략히 살펴보고, 이러한 각각의 단일 모형들을 결합하여 통합모형 구축을 시도하고자 한 기존 연구들에 대해 살펴본다. 이어 제 3장에서 제안하고자 하는 GA 기반 통합모형에 대해 설명하고, 제 4장에서는 앞서 제시한 모형을 실제 침입탐지 로그 데이터를 통해 실증 분석한 결과를 제시한다. 마지막으로 제 5장에서는 연구결과를 종합적으로 정리한 뒤, 본 연구의 한계점과 향후 연구방향을 제시한다.

2. 이론적 배경

2.1 침입탐지시스템 및 비대칭 오류비용

컴퓨터에서 사용 및 활동되어 있는 자원의 무결성, 비밀성, 가용성을 방해하는 일련의 행위이자, 컴퓨터 및 네트워크 시스템의 보안 정책을 파괴하는 행위를 침입(intrusion)이라 정의할 수 있다. 이러한 침입을 감시하고 침입여부를 인식하는 작업으

로서, 현재 기업 및 관공서 등에서 침입탐지를 자동으로 수행하고 침입발견 즉시 적절한 대응을 취할 수 있도록 설계된 정보보호 보안장비인 침입탐지시스템을 운영하고 있다(김한성 외, 2003; 박성갑, 2005). 침입탐지시스템의 목적은 네트워크상에서 실시간으로 정상적인 사용자와 침입자(해커)를 구분하는 방식으로 보안위반을 탐지하기 위한 메커니즘을 제공하는 것이다(Debar et al., 1992).

침입탐지시스템에 있어 다음 아래의 두 가지 유형의 오류는 필수적인 형태이다. 먼저 첫 번째 오류인 False-Positive Error(이하 FPE)는 침입탐지시스템이 정상 패킷을 비정상으로 잘못 판단하여 발생하는 오류로서, 이 경우 해당 기업 및 관공서에서는 오류에 따른 불필요한 조치를 취하게 된다. 두 번째 유형인 False-Negative Error(이하 FNE)는 침입탐지시스템이 악의적인 공격이나 비정상적인 패킷을 정상으로 잘못 판단하는 오류로서, 일반적으로 FPE보다 FNE가 훨씬 치명적이다. FPE와 FNE의 산출식은 아래와 같다(엄남경 외, 2006; 이현욱, 안현철, 2011).

$$\text{FPE}(\%) = \frac{\text{침입으로 분류된 정상 데이터 수}}{\text{전체 정상 데이터 수}} \times 100$$

$$\text{FNE}(\%) = \frac{\text{정상으로 분류된 침입 데이터 수}}{\text{전체 침입 데이터 수}} \times 100$$

앞에서 언급한 것처럼 FPE가 발생할 경우, 네트워크를 운영하고 있는 기업이나 관공서에서는 해당 패킷에 대해 불필요한 대처방안을 계획 및 수립하여 시행하게 되고 또한 정상 업무를 방해하는 등 각 기관의 생산성을 감소시키는 등의 기회비용을 유발하게 된다. FNE가 발생할 경우에는, 비정상을 정상으로 오분류 하기 때문에 네트워크 침입으로 인한 직접적인 피해가 발생될 수 있으며 이 경우 상황에 따라 해당 조직에 엄청난 피해 및 손실을 유발할 수 있다(홍태호, 김진완, 2005; 홍태호, 김진완, 2006; Joo, et al., 2003; Lee and Kim, 2006). 때문에 일반적으로 FPE 보다는 FNE를 보다 효과적으로 통제할 수 있는 침입탐지시스템이 더 높은 실용적 가치를 지니게 되는 것으로 평가된다.

2.2. LOGIT

LOGIT은 기업부도예측, 고객분류 등을 위한 평가를 위한 연구에 많이 사용되고 있는 모형으로 통계적인 분석방법을 활용한다. 예를 들어, 본 연구에서 다루고 있는 침입탐지시스템의 경우, IDS 센서로부터 수신된 패킷이 정상인지 혹은 비정상인지에 대해 예측할 수 있어야 한다. 분류기준값이 0.5보다 크면 침입이라 분류하고 분류기준값이 0.5 이하이면 정상이라 분류할 수 있다. 이처럼 이항확률을 가진 종속변수를 통계적으로 설명하고자 할 때, 일반적인 회귀분석에서는 종속변수를 연속변수의 형태를 가정하는데 반해, 이러한 분류의 문제에서는 종속변수가 이항변수이므로 오차의 분포가 정규분포를 따라야 한다는 회귀분석의 일반적인 가정에 위배되기 때문에 일반적인 회귀분석은 적용하기 어렵다. 또한 일반적인 회귀분석을 사용할 경우에는 종속변수가 $-\infty \sim +\infty$사이의 모든 값을 가질 수 있는데, 이항 확률을 갖도록 하기 위해서는 종속변수 값의 범위를 0~1까지 제한시켜야 한다. 이러한 문제들을 해결하기 위해 사용되는 기법이 바로 LOGIT이다(김수영, 2006; 박정민, 2003; 안현철 외, 2005). 하나의 입력 변수가 다른 변수들에 의해 설명 또는 예측되는지를 알아보기 위해서 LOGIT은 각 자료를 함수식으로 표현하여 분석하는 통계적인 방법으로 두 개 또는 그 이상의 값을 가지는 변수를 예측하는데 사용될 수 있으나 일반적으로 두 개의 값만을 가지는 변수에

대한 예측모형에 주로 사용하게 된다(이형용, 2008).

LOGIT은 회귀분석과 같은 통계기법에 기반하고 있음으로 모형 산출이 비교적 단순하고 모형에 대한 해석이 용이하다는 장점이 있다. 하지만, 통계모형에 기반하고 있어 복잡한 비선형 패턴을 모형에 표현할 수 없다는 점과 그로 인해 일반적으로 다른 기법들에 비해 예측성과가 다소 떨어진다는 단점이 있다(이현욱, 안현철, 2011).

2.3 DT

DT는 의사결정규칙을 도표화하여 관심 대상이 되는 집단을 몇 개의 소집단으로 분류하거나 예측을 수행하는 분석기법이다. 이 기법은 분류 또는 예측의 과정이 나무구조에 의해 도표화 되는 추론규칙이기 때문에, ANN이나 판별분석, 회귀분석 등과 같은 단일 모형들에 비해, 그 과정을 쉽게 이해하고 설명할 수 있다는 장점이 있다(김성준, 2003; 이승태, 김성신, 2005). 또한 이해하기 쉬운 규칙을 생성시켜 주기 때문에 분류작업이 다소 용이하고 가장 좋은 변수를 명확히 알아낼 수 있는 장점도 있다(이현욱, 안현철, 2011).

이러한 DT 분석을 위한 대표적인 알고리즘으로는 CHAID(Kass, 1980), CART(Breiman et al., 1984), C4.5(Quinlan, 1993) 등이 있다. 먼저 CHAID (Chi-squared Automatic Interaction Detection) 기법은 최적의 분리기를 찾기 위해 카이제곱(χ^2) 분포를 사용한다. 구체적으로, CHAID 기법의 경우 연속형 예측변수는 구간별로 그룹화하여 범주형으로 변환시킨 후에, 각각의 예측변수와 목표변수의 분할표로 부터 카이제곱 통계량을 측정하는 것이다. 이를 통해 모든 예측 변수에 대해 카이제곱 통계량을 구하고, 이 가운데 가장 유의한 변수를 선택하여 분리변수로 사용하게 된다. 또한 CHAID에서는 분리변수의 각 범주가 하나의 부마디를 형성하는 다원 분리를 실행한다. 반면 CART(Classification and Regression Tree)는 전체 탐색법을 통해 최선의 이진 분리를 찾는 방식으로 가장 널리 사용되는 의사결정나무 알고리즘이다. 각각의 마디에서, 모든 가능한 분리에 대하여 불순도를 측정하고, 이 불순도가 최소로 되는 분리 기준을 선택하는 것이다. 이 때, 불순도의 지표로는 지니(Gini) 측도가 가장 많이 사용된다(이현욱, 안현철, 2011).

하지만 최근에는 이러한 알고리즘간의 구별이 모호해지면서 여러 상용 데이터마이닝 패키지들이 기존의 알고리즘들을 결합하고 확장하여 다양한 분석을 수행할 수 있는 기능을 제공하고 있다(안현철, 2002). 하지만 나무가 도표가 너무 깊은 경우에는 과적합화로 인해 예측력이 저하될 수 있고, 해석하기가 쉽지 않으며 목표변수가 연속형인 모형에서는 그 예측력이 다소 떨어진다는 한계가 존재한다.

2.4. ANN

ANN은 인간의 생물학적인 뇌의 기능과 작동원리를 기반으로 한 인공지능 기법으로, 우수한 예측력으로 인해 오늘날 경영학뿐만 아니라 금융분야에서도 활용되고 있으며 재무, 회계, 마케팅, 생산 등의 다양한 분야에서 적용되고 있는 있다. 특히, 재무분야에 관한 응용연구에서는 주가지수예측, 신용등급 예측, 이자율 예측 등 다양한 분야에서 활용되고 있다(안현철 외, 2005; 이형용, 2008; 이현욱, 안현철, 2011).

ANN을 구성하는 가장 기본적인 구성단위는 처리요소(PE, processing element)인데, 동시에 혹은 병렬적으로 작동하는 처리요소들은 한 곳에 모여서 하나의 층을 형성한다. 이러한 층의 관점에서,

보통의 ANN은 입력층, 은닉층(중간층), 출력층의 3가지 층을 갖게 된다. 은닉층 또는 중간층은 ANN이 비선형 문제의 해결을 가능케 하는 주요한 요인이며 문제의 특성에 따라 존재하지 않을 수도 있고, 하나 혹은 그 이상의 은닉층을 가질 수도 있다. ANN은 복잡하고, 비선형적인 자료에서 지식이나 패턴을 추출할 수 있고, 입력-출력 사상(input-output mapping) 기법이라서 자료에 대한 통계적인 분석 없이 결정을 수행할 수 있으며, 상대적으로 적응력이 뛰어나고 견고한 모형이라는 점이 장점이다. 즉, 불완전한 입력정보를 가지고도 적정한 결과를 생성할 수 있으며 새로운 환경에서 학습수행이 가능하다는 장점이 인공신경망의 주요 장점이라고 할 수 있다(심홍기, 김승권, 2008; Fletcher and Goss, 1993; Kim and Lee, 2004).

그러나, 다른 한 편으로는 많은 문제점들로 인해 비판을 받기도 한다. 우선, 블랙박스 모형화(black box modeling)라고 비판 받는 문제, 즉 모형이 제시하는 최종 결과에 대해서는 왜 그런 결과가 나오는지에 대한 원인을 충분히 설명할 수 없다는 점과 과도하게 학습모형을 진행시킬 경우, 전체적인 관점에서의 최적해가 아닌 지역적인 관점에서의 최적해가 선택될 수 있다는 과적합화 문제는 ANN의 가장 치명적인 단점이라고 할 수 있다(이현욱, 안현철, 2011; Berry and Linoff, 1997). 아울러, 학습에 많은 표본이 요구된다는 문제, 모형 설계 시 설계자의 직관에 의해 설정되어야 하는 파라미터(parameter)들이 과도하게 많다는 문제 등도 ANN의 주요 문제점으로 지적될 수 있다.

2.5 SVM

SVM은 러시아의 통계학자인 Vapnik(1998)에 의해 처음 소개된 기계학습알고리즘 기법으로, 입력공간과 관련된 비선형 문제를 고차원의 특징공간의 선형문제로 사상(mapping)시켜 나타내기 때문에 수학적으로 분석하는 것이 수월하다는 장점이 있다(Hearst et al., 1998). 또한 SVM은 ANN과 달리 조정해야 할 파라미터의 수가 그리 많지 않아 비교적 간단하게 학습에 영향을 미치는 요소들을 규명할 수 있다. 그리고 구조적 위험을 최소화함으로써 ANN의 치명적인 한계로 지적되어 온 과적합화 문제에서 벗어날 수 있다. 또한 블록함수를 최소화하는 학습을 진행하기 때문에 지역적인 해가 아닌 전체적인 전역 최적해를 구할 수 있다는 점에서 ANN보다 성능이 좋은 기계학습기법으로 주목 받고 있다(안현철 외, 2005; 안현철, 이형용, 2009; 이현욱, 안현철, 2011).

이러한 장점을 기반으로 최근에는 SVM을 활용한 다양한 연구가 진행되고 있다. 그 예로서 문서분류, 영상인식, 문자인식, 신용평가, 주가예측, 구매고객 예측 등의 분야에서 SVM은 뛰어난 일반화 성능을 보여주었다(김선웅, 안현철, 2010; 박정민, 2003; 안현철 외, 2005; Joachims, 1998; Osuna et al., 1997). SVM은 훈련 데이터들을 서로 다른 두 개의 집단으로 분류할 때, 분류의 기준이 되는 분리 경계면(hyperplane)을 학습 알고리즘을 이용하여 찾는 원리로 이루어진다(이수용, 이일용, 2002). 구체적으로, SVM은 입력벡터를 고차원의 특징공간으로 사상시킨 후 두 분류집단 사이의 여백을 최대화시키는 분리 경계면을 찾는 것을 목적으로 한다. 이러한 최대 마진 분리 경계면은 두 분류집단 사이의 최대 거리로 분리하는데 이때 최대 마진 결정함수에 가장 근접한 훈련 데이터를 서포트 벡터(support vector)라고 부른다(김선웅, 안현철, 2010; 안현철 외, 2005). SVM에 아무리 많은 훈련 데이터가 제공된다고 하더라도, 결국 최종 모형은 소수의 서포트 벡터만을 이용해서 도출되기 때문

에, 학습에는 많은 훈련 데이터를 필요로 하지 않는다.

SVM은 기본적으로 두 집단을 가장 잘 분류할 수 있는 분류기를 찾도록 설계되어 있기 때문에 본래의 SVM 기법을 이용할 경우, 분석의 대상이 되는 데이터가 어느 집단에 속하는지에 대해서는 예측할 수 있지만, 각각의 집단에 어느 정도의 확률로 속해 있는지에 대해서는 산출하지 못한다는 단점이 있다. 이를 개선하기 위해 Platt(2000)은 SVM의 집단별 추정 소속확률을 산출할 수 있는 방법을 제안하였으며, 집단별 추정 소속활률을 산출하는 기법은 지금까지도 다양한 연구에서 활용되고 검증되어 왔다(Sollich, 2002; 홍태호, 신택수, 2005; 김선웅, 안현철, 2010 등).

2.6 통합모형에 관한 연구

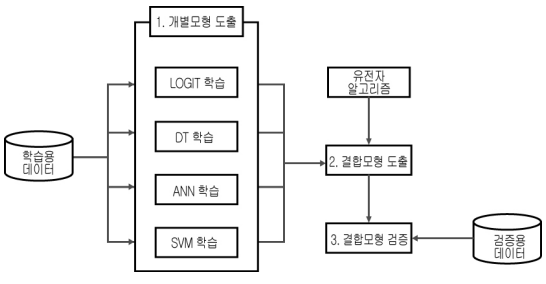
여러 가지 다른 단일기법들의 모형 결과들을 통합하면 한 가지 기법을 통해서 얻을 수 있는 우수한 결과 보다 각 기법들의 통합된 모형이 더 우수한 예측성능을 보여주기 때문에 통합모형 방법론이 중요시됨을 알 수 있다. 앙상블 기법을 대부분의 모형을 통합하는 기법으로 사용한다. 이 앙상블 기법은 각각의 모형 결과들을 단순 평균하거나 투표, 또는 설정 기준을 조정하는 방법이다. 그러나 최근에는 서로 다른 단일기법들의 결과를 최적화하고 통합하여 단일보다 더 정확한 예측 결과를 산출 할 수 있는 통합모형 방법론이 제기되고 있다(이형용, 2008).

모형 통합에 관한 기존 연구로는 Han et al.(1997)은 기업도산 예측 연구에서 판별분석, LOGIT, ANN 모형의 결과값을 GA를 적용하여 가중치를 산출하였고 산출된 각 기법들의 결과들을 통합, 적용하여 모형통합의 우수성을 입증하였다. 이 연구에서 다른 모형들에 의해 산출된 결과들을 결합하면 결합된 모형의 예측성과 및 우수성이 기업도산 예측 분류의 성능을 더 높인다는 것을 제시하였다.

김경재, 한인구(2001)는 기존의 인공신경망 모형에 퍼지 개념을 통합하여 신경망 학습에 쓰이는 자료를 퍼지화하였으며 홍승현, 신경식(2003)은 GA 이용하여 기업부도예측의 입력 변수를 선정하여 각각의 인공신경망 모형을 하나의 통합된 인공신경망 통합 모형을 제시하기도 하였다. 이형용(2009)와 안현철, 이형용(2009)은 GA 기반한 여러 모형의 결합가중치를 고려한 통합모형을 제시하여 주가지수를 기반한 투자 의사결정지원 모형에 적용하여, 주가지수 예측 성과의 우수성을 실증 및 분석하였다.

3. 비대칭 오류비용을 고려한 GA 기반 침입탐지 모형

본 연구는 GA 기반 통합모형을 활용하여, 비대칭 오류비용을 고려한 새로운 지능형 침입탐지 모형을 제안한다. 본 연구의 제안모형은 ANN 모형에 비대칭 오류비용을 반영하여 침입탐지모형을 개선하고자 한 기존문헌 Joo et al.(2003)의 연구에 근간하고 있다. 다만, Joo et al.(2003)의 연구와는 달리, 침입탐지모형의 핵심이 되는 분류기법을 각각의 단일모형들을 결합하는 GA 기반 통합모형으



<그림 1> 연구모형 구성

로 설정하였다는 점에서 기존 연구와 차이가 있다고 할 수 있다. 본 연구의 핵심이 되는 제안모형을 <그림 1>과 같이 제시하였다.

상단의 <그림 1>에 제시된 바와 같이, 우선 공공분야 IDS 센서로부터 수집된 로그 데이터를 표본 추출하게 되는데, 이 때 정상 데이터와 비정상 데이터의 비율이 1:1이 되도록 무작위 표본 추출을 수행하게 된다. 이러한 과정을 통해 수집된 로그 데이터는 다시 학습용 데이터와 검증용 데이터로 구분되며, 이 중 학습용 데이터를 이용해 단일모형의 분류기법에 대한 모형에 학습된다. 본 연구에서 분류기법으로는 침입탐지모형에 적용 가능한 총 5가지 분류기법들-즉, LOGIT, DT, ANN, SVM과 GA 기반 통합 모형-을 모두 적용해 보도록 하였으며, 검증용 데이터에 적용해 보았을 때, 과연 '오판률' 관점에서 본 연구에서 제안하는 GA 기반 통합모형이 실제로 가장 우수한 예측성과를 보이는지 먼저 확인해 보도록 한다.

최적의 예측모형이 확인 및 선택되면 이후에는 FPE와 FNE의 서로 다른 상황을 가정한 10가지의 시나리오에 따라, 전체 오분류 비용을 최소화하는 최적의 분류기준 값을 탐색하는 과정이 이루어지게 된다. 이 때 시나리오는 Joo et al.(2003)의 연구를 참고하여, FNE와 FPE의 간 상대적 비율을 다르게 설정한 총 10가지의 시나리오를 사용하였다.

4. 실험 및 결과

4.1 데이터 및 성능평가 기준

본 연구의 제안모형을 검증하기 위해, 실제 침입탐지시스템으로부터 확보된 데이터를 이용한 실증분석을 시도하였다. 실험에 사용된 데이터는 국내 한 공공기관의 IDS 센서로부터 수집된 로그 데이터이다. 해당 공공 기관으로부터 본 연구의 모델링을 위해 확보한 데이터는 2010년 1월부터 6월 사이에 수집된 약 15,000여건의 로그 데이터인데, 이 중 10,000건의 데이터를 무작위 표본 추출하여 실험에 활용하였다. LOGIT과 DT의 실험은 PASW Statistics v18.0을 사용하였으며 ANN의 실험 경우는 Neuroshell R4.0을, SVM의 실험 경우는 LIBSVM v2.9를 사용하였다. 그리고 통합모형은 Microsoft Excel 2007의 VBA(Visual Basic for Application) 프로그램을 활용했으며 GA 최적화를 위한 탐색의 경우 Palisade Software사의 Evolver Industrial 5.5를 사용하였다.

침입탐지모형을 위한 LOGIT, DT, ANN, SVM의 입력변수들은 문헌 연구 및 전문가와의 델파이 연구기법을 통해 아래의 <표 1>과 같이 선정하였다. 이 중, 공휴일 여부, 일과시간 여부와 같은 파생변수들은 기존 연구들에서 사용된 입력변수가 아니지만, 전문가들의 조언을 통해 새로 추가된 입력변수들이다. GA 통합모형에서 최적화의 대상이 되는 변수는 4개 단일모형의 가중치로 선정하였다. 즉, LOGIT, DT, ANN, SVM의 단일 예측결과가 GA 기반 통합모형의 입력변수가 된다. 아울러, IP 주소의 경우 기존 연구의 사례를 참고하여, 주소를 구성하는 4개의 클래스를 각각 개별 입력변수로 구성하여 입력변수로 사용하였다.

<표 1> 변수 및 설명

변수 명	설명
Workday	토・일요일, 공휴일과 근무일 구분
Overtime	일과이전/이후 시간 구분
Source IP	출발지 IP 주소(4개 클래스 구분)
Source Port	출발지 Port 번호
Destination IP	목적지 IP 주소(4개 클래스 구분)
Destination Port	목적지 Port 번호
Protocol	프로토콜 유형(1 : TCP, UDP/0 : ICMP)

연구모형의 1단계에서, 5가지 분류기법의 우수성을 평가하기 위한 기준으로는 전체적인 예측정확도를 사용하였다. 즉, 1단계의 우수성 평가에서는 FNE, FPE를 구분하여 고려하지 않고, 전체 예측대상 사례 중 정상을 정상으로, 혹은 비정상을 비정상으로 정확하게 판단한 사례의 비율을 계산하여, 이를 분류기법의 우수성을 평가하는 기준으로 사용하였다. 그런 다음 2단계에서는 전체 오분류 비용을 기준으로 하여, 본 연구에서 제안하는 GA 기반 통합모형과 단일 모형 중 지금까지 가장 많이 사용되어 온 ANN 및 SVM 모형을 서로 비교해 보는 형태로 진행하였다.

또한 학습용 데이터로는 전체 데이터의 80%에 해당되는 8,000건의 데이터를, 검증용으로는 전체 20%에 해당되는 2,000건의 데이터를 사용하였다. 다만, ANN의 경우 과적합화를 피하기 위해, 학습용 데이터를 다시 3 : 1의 비율로 나누어, 모형구축용 데이터 6,000건과 과적합 여부 확인용 데이터 2,000건으로 나누어 사용하였다.

4.2 1단계 : SVM을 비롯한 분류 모형 구축

전술했듯이, 1단계에서는 본 연구에서 제안하는 GA 기반 통합모형의 우수성을 확인하기 위한 비교모형으로 LOGIT, DT, ANN, SVM을 함께 적용해 본다. 제안모형의 성과를 보다 정확하게 검증하기 위해서 본 연구에서는 다음의 <표 2>와 같은 다양한 단일모형의 비교모형들을 설정하였다. 전술했듯이, 1단계에서 GA의 적합도 함수는 학습용 데이터에 대한 오판률, 즉 예측 정확도(hit ratio)로 설정하고 실험하였다. GA 기반 통합모형에서 최적화된 각 기법들의 가중치는 다음의 <표 2>와 같다.

<표 2> GA 기반 통합모형에서 도출된 각 기법들의 가중치 비중

모형	Weight(0～127) : 7bit	비중
LOGIT	0	0.00
DT	127	0.45
ANN	58	0.20
SVM	98	0.35

위의 <표 2>는 GA가 탐색한 각 기법들의 가중치 결과를 나타내고 있다. 여기 도출된 최적의 GA 기반 통합모형 구현 시 가중치 비중을 보면, LOGIT는 영향력이 거의 없음을 알 수 있고, 반면 DT에 의존하는 경향은 상당히 높다는 것을 확인할 수 있다. 또한 ANN과 SVM의 비중을 합쳐 약 55% (0.55) 정도를 보이고 있음을 알 수 있는데, 이는 본 연구의 대상이 되고 있는 침입탐지 분야가 상당히 비선형의 특성이 높은 패턴을 보이는 영역이라는 점을 시사한다고 해석할 수 있다. 예측정확도를 기준으로, 앞서 소개한 본 연구의 제안모형과 비교모형으로 설정한 4개 단일모형들의 성과를 비교한 결과, 다음의 <표 3>과 같은 결과를 얻을 수 있었다.

<표 3> 단일 및 통합모형의 예측 정확도

모형	예측 정확도(%)		
	학습용	테스트용	검증용
LOGIT(forward)	85.71	.	85.30
DT(CHAID)	96.34	.	96.55
ANN(h = 11)	96.00	96.85	96.80
SVM	97.49	.	96.90
GA 기반 통합모형	97.93	.	97.90

위의 <표 3>에서 보는 바와 같이 예상대로 GA 기반 통합모형이 타 모형에 비해 가장 우수한 성과를 보이고, 이어 SVM의 성과가 우수한 이분류 예측성과를 보이고 있음을 확인할 수 있다. 전체적인 예측성과를 볼 때, LOGIT 예측정확도가 80%

대의 비교적 낮은 예측력을 보이는데 반해 DT, ANN, SVM과 GA 기반 통합모형은 90%대의 상대적으로 우수한 예측력을 보이고 있음을 알 수 있다.

우리가 제안하는 GA 기반 통합모형은 학습용 및 검증용 데이터 모두에서 비교하고자 하는 단일 기법에 기반한 모형보다 더 우수한 예측력을 보임을 확인할 수 있다. SVM과 비교하였을 경우 학습용은 0.44% 차이가 나며 검증용은 1.00%의 차이가 나타남을 확인할 수 있다. 수치상으로는 차이가 크게 나지 않지만 실험한 IDS의 로그 데이터 10,000건의 대해서, 1.0%는 100건의 로그 데이터를 의미한다. 따라서 100건의 로그 데이터에 대해 제안하는 GA 기반 통합모형이 SVM 보다 훨씬 우수한 정확도를 가진 것을 확인할 수 있었다.

아울러, ANN보다는 SVM이, SVM보다 GA 기반 통합모형이 다소나마 더 우수한 능력을 갖고 있음을 본 실험결과를 통해 확인할 수 있다. 이는 <표 2>의 결과와 정확하게 연결되며, 우리가 찾아내려고 하는 침입 패킷의 패턴이 상당히 높은 비선형적인 특성을 갖고 있음을 시사하고 있다 하겠다.

4.3 2단계 : 분류기준 값 최적화를 통한 ANN, SVM과 GA 기반 통합모형 도출

전술한 바와 같이, 본 연구에서는 GA를 이용해 연속된 예측값을 생성할 수 있는 4가지 기법-즉 LOGIT, DT, ANN 그리고 SVM-의 예측결과를 결합하여, 보다 우수한 예측결과를 생성시킬 수 있는 새로운 통합모형을 제안하고 있다. 제안하는 GA 기반 통합모형의 우수성을 확인하기 위해 비교모형으로 ANN, SVM을 함께 적용해 본다. 초기 분류기준 값으로는 앞서 언급한대로 0.5를 사용한다. 하지만, 0.5로 설정되는 일반적인 분류기준 값은 기본적으로 FPE와 FNE로 인해 발생하는 비용을 전혀 고려하지 않기 때문에, 비용의 관점에서 최적이 아닐 가능성이 크다. 기본적으로 FPE와 FNE는 서로 절충관계(trade-off)에 있는데, 분류기준 값이 0에 가까워질수록 FPE는 늘어나는 반면, FNE가 감소하게 되고, 반대로 분류기준 값이 1에 가까워질수록 FPE는 감소하는 반면, FNE는 증가하게 된다.

따라서 FPE와 FNE로 인해 발생하는 비용이 상대적으로 어떻게 차이가 나는가에 따라, 최적의 분류기준값, 즉 최적 임계치는 달라질 수 있다. 결국, 비대칭 오류비용을 고려한다는 것은 FPE와 FNE의 비용이 서로 다르다는 전제 하에서부터 출발해, 한 쪽의 오류를 다른 쪽의 오류보다 더 통제, 관리하겠다는 것을 의미한다. 그리고 이 때 오류를 통제하는 방법으로는 기준이 되는 '임계치'의 조정이 사용된다.

ANN, SVM, GA 통합모형의 전체 오류비용은 다음 식에 의해 산출된다.

$$\text{Total Cost} = \frac{w_1 \cdot \text{FPE} + w_2 \cdot \text{FNE}}{w_1 + w_2}$$

결국 전체 오류비용은 FPE와 FNE의 상대적 가중치, 즉 w_1과 w_2를 어떻게 설정하는가에 따라 달라질 수 있다. 이에 우선 $w_1 = w_2 = 1$인 가장 기본적인 상황을 상정하여, 전체 비용을 최소화하는 최적의 분류기준값을 탐색해 보았다. 이 때, 최적의 분류기준값을 탐색하기 위한 도구로는 Microsoft Excel에 Add-in 형태로 제공되는 Solver(해 찾기) 기능을 사용하였다.

실험결과, ANN, SVM, GA 통합모형 모두 전체 오류비용은 U자형의 곡선모양을 나타낸다. 즉, 분류기준 값이 너무 0에 가까워도 비용은 증가하며, 반대로 1에 가까워져도 비용은 증가하는 것이다. 0

<표 4> 특정 분류기준 값에 대한 ANN, SVM과 GA 성과 비교

데이터 구분	ANN				SVM				GA			
	FPE (%)	FNE (%)	전체비용 (%)	분류기준	FPE (%)	FNE (%)	전체비용 (%)	분류기준	FPE (%)	FNE (%)	전체비용 (%)	분류기준
학습용	5.10	2.48	3.79	t = 0.5	2.85	2.15	2.50	t = 0.5	2.58	1.58	2.08	t = 0.5
검증용	4.50	1.90	3.20		3.10	3.00	3.05		2.30	1.90	2.10	
전체	4.98	2.36	3.67		2.90	2.32	2.61		2.52	1.64	2.08	
학습용	4.58	3.23	3.90	t = 0.57	2.68	2.38	2.53	t = 0.56	2.58	1.58	2.08	t = 0.5
검증용	3.60	2.50	3.05		2.60	3.10	2.85		2.30	1.90	2.10	
전체	4.38	3.08	3.73		2.66	2.52	2.59		2.52	1.64	2.08	

에 가까워질 경우, FNE는 0으로 수렴하지만, FPE가 1로 수렴하고, 반대로 1에 가까워지면 FPE가 0으로 수렴하지만 FNE가 1로 수렴하면서 비용이 증가한다. 그 결과가 아래의 <표 4>에 제시되어 있다. ANN의 경우 분류기준 값이 0.57에서의 전체 비용이 3.05%로서 이 구간에서 가장 낮은 전체 비용을 보이는 반면, SVM의 경우 분류기준 값이 0.56에서의 전체 비용이 2.85%로서 이 구간에서 가장 낮은 전체 비용을 보이고 있다. 한편 GA의 경우 분류기준 값이 0.5에서 전체 비용이 2.1%로 가장 낮은 전체 비용을 보이고 있다.

또한, <표 4>에서 볼 수 있듯이, FPE와 FNE의 가중치가 1 : 1로 동일하다고 가정할 경우 ANN은 분류기준 값이 0.57일 때, SVM은 분류기준 값이 0.56일 때, GA는 분류기준 값이 0.5일 때, 전체 비용이 가장 최소화되었음을 알 수 있었다.

위의 <표 4>를 통해 우리는 학습용 데이터, 검증용 데이터, 그리고 전체 데이터 기준 모두에서 GA 통합모형이 SVM, ANN보다 항상 오류비용이 더 작게 나타나고 있음을 알 수 있다. 아울러, SVM은 ANN보다 항상 오류비용이 더 작게 나타남을 알 수 있다. 이를 통해, 비대칭 오류비용의 관점에서는 「GA 통합모형 > SVM > ANN」 순으로 성과의 개선효과가 나타남을 확인할 수 있다.

<표 5> FNE의 가중치 변화에 따른 SVM, ANN, GA 통합모형 성과 비교

No	w_1	w_2	ANN(%)				SVM(%)				GA(%)			
			FPE	FNE	Total Cost	TC 변동률	FPE	FNE	Total Cost	TC 변동률	FPE	FNE	Total Cost	TC 변동률
1	1	1	3.60	2.50	3.05	0.00	2.60	3.10	2.85	0.00	2.30	1.90	2.10	0.00
2	1	2	6.30	0.80	2.63	-13.77	4.70	2.00	2.90	1.75	3.90	0.70	1.77	-15.71
3	1	3	6.30	0.80	2.18	-28.52	8.20	0.30	2.28	-20.00	3.90	0.70	1.50	-28.57
4	1	4	7.00	0.60	1.88	-38.36	8.20	0.30	1.88	-34.04	3.90	0.70	1.34	-36.19
5	1	5	7.00	0.60	1.67	-45.25	8.20	0.30	1.62	-43.16	3.90	0.70	1.23	-41.43
6	1	6	7.00	0.60	1.51	-50.49	8.20	0.30	1.43	-49.82	3.90	0.70	1.16	-44.76
7	1	7	7.00	0.60	1.40	-54.10	8.20	0.30	1.29	-54.74	6.30	0.30	1.05	-50.00
8	1	8	7.00	0.60	1.31	-57.05	8.20	0.30	1.18	-58.60	6.30	0.30	0.97	-53.81
9	1	9	7.00	0.60	1.24	-59.34	8.20	0.30	1.09	-61.75	6.30	0.30	0.90	-57.14
10	1	10	7.00	0.60	1.18	-61.31	8.20	0.30	1.02	-64.21	6.30	0.30	0.85	-59.52

이상의 실험결과는 FPE와 FNE으로 인해 발생하는 비용이 동일하다는 가정 하에 수행된 것이다. 하지만, 일반적으로 FNE는 FPE보다 조직에 훨씬 치명적인 피해를 입힐 수 있기 때문에, 전체 비용에서 FNE에 대한 가중치(w_2)를 FPE에 대한 가중치(w1)보다 더 높게 설정하는 것이 합리적이다 (이현욱, 안현철, 2011).

이에, 본 연구에서는 FNE에 대한 가중치가 FPE에 대한 가중치보다 더 높게 부여되는 시나리오들을 설정해 보고, 해당 시나리오 별로 전체 비용을 최소화하는 최적 분류기준 값을 탐색하는 실험을 수행하였다. FNE의 가중치가 FPE의 가중치보다 1~10배로 변화하는 총 10가지 시나리오를 설정하고, 각 시나리오에 따른 최적 FPE, FNE 값과 이 때 발생되는 전체 비용을 산출해 보았다. 그 결과가 아래의 <표 5>에 제시되어 있다.

위의 <표 5>에 제시된 결과에서 볼 수 있듯이, 전체 오류비용의 경우, SVM은 시나리오 2, 3, 4의 3가지 경우를 제외하고는 ANN보다 항상 낮은 값을 산출하고 있음을 볼 수 있고 GA 통합모형의 경우 10가지 시나리오 모두 ANN, SVM보다 우수한 것으로 나타났다. 이러한 결과로 미루어 볼 때, 비대칭 오류비용을 고려할 경우에도 침입탐지모형을 GA 통합모형에 기반을 두어 설계하는 것이 ANN, SVM을 기반으로 하는 것보다 훨씬 더 유리하다는 것을 본 실험에서 알 수 있다.

5. 결론

본 연구에서는 비대칭 오류비용을 고려한 GA 기반의 통합모형인 지능형 침입탐지모형을 제안하였고, 제안 모형의 유용성을 국내 공공기관으로부터 수집한 실제 IDS 로그 데이터를 이용해 검증해 보았다. 본 연구에서 제안하는 GA의 경우, 주가지수예측, 기업신용평가 등 지금까지 다양한 분야에서 활발하게 응용되고 있는 기법으로, 여러 기법들을 결합하는데 지금까지 많이 활용되어 왔다. 하지만, GA에 기반한 통합모형은 지금까지 침입탐지 분야에 적용되지 않았으며 또한, 비대칭 오류비용을 고려하는 시도에도 도입되지 못했다.

본 연구에서 제안 모형을 실제 로그 데이터를 통해 검증해 본 결과, 예상대로 GA 기반 통합모형이 ANN이나 LOGIT이나 DT는 물론, 지금까지 주로 사용되어 온 SVM에 비해서도 훨씬 우수한 예측력을 보임을 확인할 수 있었다. 특히, 기존에 비대칭 오류비용을 고려한 연구에서 활용되어 온 SVM, ANN과의 예측 성과를 비교해 본 결과, 거의 예외 없이 어떤 상황에서도 GA 기반 통합모형이 ANN이나 SVM보다 항상 우수한 예측 성과를 보임을 확인할 수 있었다. 이러한 본 연구는 학술적인 관점에서 볼 때 기존에 시도되지 않았던 GA 기반 통합모형과 비대칭 오류비용 최적화의 결합을 침입탐지 분야에서 처음으로 시도했다는 점에서 그 의의를 갖는다고 할 수 있다.

끝으로, 본 연구의 한계점과 향후 연구방향을 정리하면 다음과 같다. 우선, 본 연구에서 제시한 모형을 보다 타당성 있는 연구결과 도출을 위해서는 다른 공공기관의 IDS 로그 데이터를 통해 검증해 볼 필요가 있다. 또한, 본 연구는 총 13개의 입력변수를 예측모형에 사용하였는데, 추후 연구에서는 IDS에서 탐지할 수 있는 추가적인 변수들도 모형에 반영함으로써, 침입탐지모형의 예측력 개선을 도모해 볼 필요가 있다. 마지막으로, 현재 본 연구의 제안모형을 정보보호 분야의 침입탐지모형에 적용하였지만, 주가지수 상품의 투자 및 의료분야의 질병 진단 예측문제, 마케팅 분야의 표적고객 선택문제 등의 해결에도 제안모형이 충분히 적용될 수 있을 것이다. 이러한 새로운 분야에 대한

제안모형의 적용과 관련한 연구가 추후 후속연구로 진행되어야 한다.

참고문헌

김선웅, 안현철, “Support Vector Machines와 유전자 알고리즘을 이용한 지능형 트레이딩 시스템 개발”, *지능정보연구*, 16권 1호(2010), 71~92.

김성준, “의사결정나무에서 다중 목표변수를 고려한”, 한국퍼지 및 지능시스템학회 2003년도 추계학술대회 학술발표논문집, (2003), 243~246.

김수영, “다변량 판별분석과 로지스틱 회귀분석, 인공신경망 분석을 이용한 호텔 도산 예측”, *한국관광학회지*, 30권 2호(2006), 53~75.

김한성, 권영희, 차성덕, “SVM 기반의 신분위장 탐지기법”, *정보보호학회논문지*, 13권 5호(2003), 91~104.

박성갑, 통합보안관리를 위한 네트워크 기반의 국방 침입방지시스템에 관한 연구, 석사학위논문, 연세대, 2005.

박정민, Support Vector Machine을 이용한 기업부도예측, 석사학위논문, 한국과학기술원, 2003.

손태식, 서정우, 서정택, 문종섭, 최홍민, “Support Vector Machine 기반 TCP/IP 헤더의 은닉채널 탐지에 관한 연구”, *정보보호학회논문지*, 14권 1호(2004), 35~45.

심흥기, 김승권, “인공신경망을 이용한 대대전투간 작전지속능력 예측”, 지능정보연구, 14권 3호(2008), 25~39.

안현철, 데이터마이닝을 활용한 인터넷 쇼핑몰의 상품 추천 시스템 개발, 석사학위논문, 한국과학기술원, 2002.

안현철, 김경재, 한인구, “Support Vector Machine을 이용한 고객구매예측모형”, *지능정보연구*, 11권 3호(2005), 69~81.

안현철, 이형용, “투자 의사결정 지원을 위한 유전자 알고리즘 기반의 다중 인공지능 기법 결합모형”, *e-비즈니스연구*, 10권 1호(2009), 267~288.

엄남경, 우성희, 이상호, “SVM과 의사결정트리를 이용한 혼합형 침입탐지 모델”, *정보처리학회논문지*, 14권 1호(2007), 1~6.

엄남경, 우성희, 이상호, “SVM과 데이터마이닝을 이용한 혼합형 침입탐지 모델”, *한국퍼지 및 지능시스템학회 2006년도 춘계학술대회 학술발표논문집*, 16권 1호(2006), 283~286.

이수용, 이일병, “Fuzzy 이론과 SVM을 이용한 KOSPI 200 지수 패턴분류기”, 한국증권학회 제4차 정기학술발표회논문집, (2002), 787~809.

이승태, 김성신, “의사결정나무를 이용한 생물의 행동 패턴 구분과 인식”, 한국퍼지 및 지능시스템학회 2005년도 추계학술대회 학술발표논문집, 15권 2호(2005), 225~228.

이영찬, “인공신경망과 Support Vector Machine의 기업부도예측 성과 비교”, 2004년도 한국지능정보시스템학회 춘계학술대회논문집, (2004), 211~218.

이종혁, 한영주, 정태명, “신경망을 적용한 침입탐지시스템의 설계”, 제21회 한국정보처리학회 춘계학술발표대회논문집, 11권 1호(2004), 1~4.

이현욱, 안현철, “비대칭 오류비용을 고려한 분류기준값 최적화와 SVM에 기반한 지능형 침입탐지모형”, 지능정보연구, 17권 4호(2011), 157~173.

이형용, “한국 주가지수 등락 예측을 위한 유전자 알고리즘 기반 인공지능 예측기법 결합모형”, *Enture Journal of Information Technology*, 7권 2호(2008), 33~43.

한국인터넷진흥원, 2010 해킹 · 바이러스 현황 및 대응(KISA-RP-2010-0051), 2011.

홍태호, 김진완, “데이터마이닝의 비대칭 오류비용을 이용한 지능형 침입탐지시스템 개발”, *정*

보시스템연구, 15권 4호(2006), 211~224.

홍태호, 김진완, "침입탐지시스템이 비대칭 오류비용을 이용한 데이터마이닝의 적용전략", 한국지능정보시스템학회 추계학술대회논문집, (2005), 251~257.

홍태호, 김진완, 김유일, "데이터마이닝 기법을 활용한 침입탐지시스템에 관한 연구", 대한산업공학회/한국경영과학회 2004 춘계학술대회, SA7-10~SA7-13, 2004.

홍태호, 신택수, "Using Estimated Probability from Support Vector Machines for Credit Rating in IT Industry", 한국지능정보시스템학회-웹코리아포럼 2005 공동추계정기학술대회, (2005), 509~515.

Berry, M. J. A. and G. Linoff, "Data Mining Techniques : For Marketing, Sales and Customer Support", Wiley Computer Publishing, 1997.

Breiman, L., J. Friedman, R. Olshen, and C. Stone, "Classification and Regression Trees. Champman and Hall", New York, NY, 1984.

Chen, R.-C., K.-F. Cheng, Y.-H. Chen, and C.-F. Hsieh, "Using Rough Set and Support Vector Machine for Network Intrusion Detection System", 2009 First Asian Conference on Intelligent Information and Database Systems, (2009), 465~470.

Chen, W.-H., S.-H. Hsu, and H.-P. Shen, "Application of SVM and ANN for intrusion detection", *Computer and Operations Research*, Vol.32(2005), 2617~2634.

Debar, H., M. Becker, and D. Siboni, "A Neural Network Component for an Intrusion Detection System", Proceedings of 1992 IEEE Computer Society Symposium Research in Security and Privacy, (1992), 240~250.

Fletcher, D. and E. Goss, "Forecasting with Neural networks and Application using Bankruptcy Data", *Information and Management*, Vol.24 (1993), 159~167.

Hearst, M. A., S. T. Dumais, E. Osman, J. Platt, and B. Scholkopf, "Support vector machines", *IEEE Intelligent System*, Vol.13, No.4(1998), 18~28.

Joachims, T., "Text categorization with support vector machines", Proceedings of the *European Conference on Machine Learning(ECML)*, (1998), 137~142.

Joo, D., T. Hong, and I. Han, "The neural network models for IDS based on the asymmetric costs of false negative errors and false positive errors", *Expert Systems with Applications*, Vol.25(2003), 69~75.

Kass, G. V., "An Exploratory Technique for Investigating Large Quantities of Categorical Data", *Applied Statistics*, Vol.29, No.2(1980), 119~127.

Kim, K.-j., "Financial time series forecasting using support vector machines", *Neurocomputing*, Vol.55, No.1-2(2003), 307~319.

Kim, K.-j. and W. B. Lee, "Stock market prediction using artificial neural networks with optimal feature transformation", *Neural Computing and Applications*, Vol.13, No.3(2004), 255~260.

Lee, S.-Y. and O.-S. Kim, "The network model for Detection Systems based on data mining and the false errors", *International Journal of Fuzzy Logic and Intelligent Systems*, Vol.6, No.2(2006), 173~177.

Osuna, E., R. Freund, and F. Girosi, "Training support vector machines : an application to face detection", *Proceedings of Computer Vision and Pattern Recognition*, (1997), 130~136.

Platt, J., "Probabilistic outputs for support vector machines and comparison to regularized like-

lihood methods", In A. J. Smola, P. L. Bartlett, B. Scholkopf, and D. Schuurmans, editors, Advances in Large Margin Classifiers, Cambridge, MA, 2000. MIT Press.

Quinlan, J. R., C4.5 : Programs for Machine Learning. Morgan Kaufmann Publishers, 1993.

Sollich, P., "Bayesian Methods for Support Vector Machines : Evidence and Predictive Class Probabilities", *Machine Learning*, Vol.46, No.1-3 (2002), 21~52.

Tay, F. E. J. and L. J. Cao, "Modified support vector machines in financial time series forecasting", *Neurocomputing*, Vol.48(2002), 847~861.

Vapnik, V., Statistical Learning Theory, Wiley, 1998.

Abstract

An Integrated Model based on Genetic Algorithms for Implementing Cost-Effective Intelligent Intrusion Detection Systems

Hyeon-Uk Lee* · Ji-Hun Kim** · Hyunchul Ahn***

These days, the malicious attacks and hacks on the networked systems are dramatically increasing, and the patterns of them are changing rapidly. Consequently, it becomes more important to appropriately handle these malicious attacks and hacks, and there exist sufficient interests and demand in effective network security systems just like intrusion detection systems. Intrusion detection systems are the network security systems for detecting, identifying and responding to unauthorized or abnormal activities appropriately. Conventional intrusion detection systems have generally been designed using the experts' implicit knowledge on the network intrusions or the hackers' abnormal behaviors. However, they cannot handle new or unknown patterns of the network attacks, although they perform very well under the normal situation. As a result, recent studies on intrusion detection systems use artificial intelligence techniques, which can proactively respond to the unknown threats.

For a long time, researchers have adopted and tested various kinds of artificial intelligence techniques such as artificial neural networks, decision trees, and support vector machines to detect intrusions on the network. However, most of them have just applied these techniques singularly, even though combining the techniques may lead to better detection. With this reason, we propose a new integrated model for intrusion detection. Our model is designed to combine prediction results of four different binary classification models–logistic regression (LOGIT), decision trees (DT), artificial neural networks (ANN), and support vector machines (SVM), which may be complementary to each other. As a tool for finding optimal combining weights, genetic algorithms (GA) are used. Our proposed model is designed to be built in two steps. At the first step, the optimal integration model whose prediction error (i.e. erroneous classification rate) is the least is generated. After that, in the second step, it explores the optimal classification threshold for determining intrusions, which minimizes the total misclassification cost. To calculate the total misclassification cost of intrusion detection system,

* Graduate School of Business IT, Kookmin University
** Graduate School of Business IT, Kookmin University
*** School of Management Information Systems, Kookmin University

we need to understand its asymmetric error cost scheme. Generally, there are two common forms of errors in intrusion detection. The first error type is the False-Positive Error (FPE). In the case of FPE, the wrong judgment on it may result in the unnecessary fixation. The second error type is the False-Negative Error (FNE) that mainly misjudges the malware of the program as normal. Compared to FPE, FNE is more fatal. Thus, total misclassification cost is more affected by FNE rather than FPE.

To validate the practical applicability of our model, we applied it to the real-world dataset for network intrusion detection. The experimental dataset was collected from the IDS sensor of an official institution in Korea from January to June 2010. We collected 15,000 log data in total, and selected 10,000 samples from them by using random sampling method. Also, we compared the results from our model with the results from single techniques to confirm the superiority of the proposed model. LOGIT and DT was experimented using PASW Statistics v18.0, and ANN was experimented using Neuroshell R4.0. For SVM, LIBSVM v2.90-a freeware for training SVM classifier-was used.

Empirical results showed that our proposed model based on GA outperformed all the other comparative models in detecting network intrusions from the accuracy perspective. They also showed that the proposed model outperformed all the other comparative models in the total misclassification cost perspective. Consequently, it is expected that our study may contribute to build cost-effective intelligent intrusion detection systems.

Key Words : Intrusion Detection System, Asymmetric Cost Of Errors, Genetic Algorithm, Integrated Model

저 자 소 개

이현욱

현재 국민대학교 비즈니스IT 전문대학원 박사과정에 재학 중이다. 3사관학교 전산정보학과에서 학사를 취득하고, 국방대학교 석사학위과정에서 전산정보를 전공하여 국방과학 석사를 취득하였다. 주요 관심분야는 IDS 패턴 분석, 네트워크 핸드오프 등이다.

김지훈

3사관학교 전산정보학과에서 학사를 취득하였고, 국민대학교 비즈니스IT전문대학원 석사학위를 취득하였다. 주요 관심분야는 AHP 기법을 이용한 연구분석, 정보보호 통합보안시스템(Integrated Security Systems) 등이다.

안현철

현재 국민대학교 경영대학 경영정보학부 조교수로 재직 중이다. KAIST에서 산업경영학사를 취득하고, KAIST 테크노경영대학원에서 경영정보시스템을 전공하여 공학석사와 박사를 취득하였다. 주요 관심분야는 금융, 고객관계관리 및 인터넷 보안 분야의 인공지능 응용, 정보시스템 수용과 관련한 행동 모형 등이다.