실시간 탐지를 위한 인공신경망 기반의 네트워크 침입탐지 시스템

김 태 희*, 강 승 호*

요 약

네트워크를 통한 사이버 공격 기법들이 다양화, 고급화 되면서 간단한 규칙 기반의 침입 탐지/방지 시스템으로는 지능형 지속 위협(Advanced Persistent Threat: APT) 공격과 같은 새로운 형태의 공격을 찾아내기가 어렵다. 기존에 알려지지 않은 형태의 공격 방식을 탐지하는 이상행위 탐지(anomaly detection)를 위한 해결책으로 최근 기계학습 기법을 침입탐지 시스템에 도입한 연구들이 많다. 기계학습을 이용하는 경우, 사용하는 특징 집합에 침입탐지 시스템의 효율성과 성능이 크게 좌우된다. 일반적으로, 사용하는 특징이 많을수록 침입탐지 시스템의 정확성은 높아지는 반면 탐지를 위해 소요되는 시간이 많아져 긴급성을 요하는 경우 문제가 된다. 논문은 이러한 두 가지 조건을 동시에 충족하는 특징 집합을 찾고자 다목적 유전자 알고리즘을 제안하고 인공신경망에 기반한 네트워크 침입탐지 시스템을 설계한다. 제안한 방법의 성능 평가를 위해 NSL_KDD 데이터를 대상으로 이전에 제안된 방법들과 비교한다.

An Intrusion Detection System based on the Artificial Neural Network for Real Time Detection

Kim Tae Hee*, Kang Seung Ho*

ABSTRACT

As the cyber-attacks through the networks advance, it is difficult for the intrusion detection system based on the simple rules to detect the novel type of attacks such as Advanced Persistent Threat(APT) attack. At present, many types of research have been focused on the application of machine learning techniques to the intrusion detection system in order to detect previously unknown attacks. In the case of using the machine learning techniques, the performance of the intrusion detection system largely depends on the feature set which is used as an input to the system. Generally, more features increase the accuracy of the intrusion detection system whereas they cause a problem when fast responses are required owing to their large elapsed time. In this paper, we present a network intrusion detection system based on artificial neural network, which adopts a multi-objective genetic algorithm to satisfy the both requirements: accuracy, and fast response. The comparison between the proposing approach and previously proposed other approaches is conducted against NSL_KDD data set for the evaluation of the performance of the proposing approach.

Key words : Intrusion Detection System, Artificial Neural Network, Multi-objective Genetic Algorithm, Feature selection, NSL_KDD data set

접수일(2017년 3월 8일), 게재확정일(2017년 3월 21일)

* 동신대학교 에너지융합대학 융합정보보안전공

★ 본 논문은 동신대학교 학술연구비 지원에 의하여 연구되었음.

1. 서 론

인터넷의 확산 및 네트워크 기반 시설의 고급화, 통신 기술의 발전 등으로 다양한 산업 분야에서 업무의 효율성 증대 및 비용 절감, 새로운 지식 정보의 창출 등 이루어지고 있다. 하지만 이러한 기술 발전의 이면에 개인의 이득이나 공명심 등의 이유로 선의의 사용자들에게 위협을 가하는 해킹 기술 또한 발전하고 있다. 사이버 공격은 디지털 기술의 발전과 함께 계속해서 진화하고 있는 실정이며, 실제 사이버 침해 사고에 의한 피해 규모는 자연재해로 인해 발생한 피해 규모보다 더 크다고 추정되고 있다.

사이버 침해 공격을 패킷 정보나 로그 등의 분석을 통해 실시간으로 방어하기 위한 수단의 하나로 침입탐지 시스템이 있다. 침입탐지 시스템은 방어하고자 하는 공격 방법에 따라 크게 두 가지로 분류 된다. 우선 기존에 알려진 공격들을 탐지하기 위한 오사용(misuse detection) 탐지 방식이 있다. 이 접근 방법의 특징은 사전에 정의된 규칙들을 이용해 잘 알려진 공격들을 탐지하는 방식으로 현장에서 가장 많이 사용되는 방법이다. 하지만 기존에 알려진 공격 방법들에 제한되어 있어 새로운 공격 방법에 대처하기 어려운 단점이 있다. 다른 침입탐지 방법은 이상 징후(anomaly detection) 탐지 방식이다. 이상 징후 탐지 방식은 정상인 사용 패턴을 근거로 이를 벗어난 행위를 이상 행위로 간주하는 방식으로 오사용 탐지 방식과 다르게 이전에 알려지지 않은 공격 방법에 대해서도 탐지할 수 있는 장점이 있다. 하지만 이상 징후 탐지 방식은 정상적인 사용 형태를 사이버 침해로 잘 못 판단하는 문제점이 지적되고 있다.

최근 데이터 마이닝이나 인공지능, 기계학습 방법을 침입탐지 시스템에 도입하는 방법들이 연구자들의 관심을 모으고 있다. 특히 기존에 알려지지 않은 공격 패턴을 찾고자하는 이상 징후 탐지 방식에 인공지능 기술을 도입하는 시도가 많이 이루어지고 있으며 상당히 높은 정확성을 보여주고 있다. 기계학습을 이용한 방법으로 인공 신경망[1], SVM[2] 등 다양한 방법들이 활용되었고 이들을 비교한 연구들도 제시되었다. 한편, 기계학습 방법은 사용하는 특징 집합에 성능이 크게 좌우되므로 최적 특징 집합을 찾으려는 연구들도 다양하게 시도 되어왔다. 일반적으로 특징 선택 방법은 크게 래퍼(wrapper) 방식과 필터(filter) 방식의 두 가지로 나눌 수 있다[3]. 래퍼 방식은 가능한 모든 특징 조합을 대상으로 특정 기계학습 모델에 가장 적합한 특징 조합을 탐색하는 방식이다. 개별 특징 조합에 대해 특정 기계학습 방식에 대한 학습과 평가가 개별적으로 이루어져야 하므로 많은 시간과 과적합(overfitting) 문제가 발생할 수 있다는 단점이 있다. 이에 반해 필터 방식은 개별 특징들을 특정 공격 유형들과의 관계성을 기준으로 선별하는 접근법을 사용한다. 대표적으로 개별 특징과 공격 유형 사이의 상관계수를 이용하는 방식이 있다. 이러한 필터 방식을 침입탐지 시스템의 특징 선택에 사용한 경우로는 정보 획득[4], 의존비[5], 상관 계수[6]를 이용한 연구들이 있다. 필터 방식은 특정 기계 모델을 상정하지 않으며 개별 특징에 대한 평가에도 학습이 사용되지 않으므로 많은 요구 시간이나 과적합과 같은 문제로 부터는 자유롭다. 이러한 이유로 많은 특징이 사용 가능한 침입탐지 시스템에서는 래퍼 방식 보다는 필터 방식을 이용한 연구가 많다. 하지만, 비슷한 특성을 가진 특징들이 선택(redundancy)되거나 특징 조합의 창발적(emergent) 성능이 배제되기 쉽다는 단점이 있고 실제 래퍼 방식에 비해 탐지율이 낮은 것으로 알려져 있다.

탐지율 이외에 중요한 평가 요소로는 탐지에 소요되는 시간이 있다. 실제 현장에서 사용되는 침입탐지 시스템은 엄청난 양의 네트워크 트래픽을 대상으로 이상 행위를 판별해야하므로 탐지에 소요되는 시간은 탐지율 못지않게 중요한 요구 조건이 되고 있다. 기계학습을 사용하는 이상 징후 탐지 기반의 침입탐지 시스템의 경우 탐지 시간과 직접적인 연관이 있는 요소는 사용하는 특징조합의 길이이다. 즉, 특징 조합의 길이가 짧을수록 학습 시간이나 탐지 시간에 적은 시간을 요구하게 된다. 하지만 일반적으로 특징 조합의 길이가 짧으면 탐지율은 떨어지는 것으로 요구 시간과 탐지율 사이에는 상충관계(tradeoff)가 있어 이를 모두 만족시키는 특징조합을 찾는 것이 중요한 문제가 되고 있다.

본 논문은 6가지 서비스 거부 공격(Denial of Service: DoS) 을 대상으로 인공신경망을 활용한 이상 징

후 탐지 기반의 침입탐지 시스템을 설계하고자 한다. 이때 탐지율과 실시간성 모두를 보장하기 위해 다중 목적 유전자 알고리즘을 사용해 특징 조합을 찾는 방법을 제안한다. 제안하는 특징 선택 방법은 래퍼 접근 방식과 유사하지만 학습에 걸리는 시간과 과적합 문제 모두를 피하기 위해 클러스터링의 정확성을 이용하는 목적함수를 정의하는 특징이 있다. 제안 방법의 성능을 측정하기 위해 NSL_KDD 데이터를 사용하고 기존에 제시된 래퍼 방식들과 탐지율 및 학습시간, 테스트 시간 등에서 비교한다.

논문의 구성은 다음과 같다. 우선 2장에서 NSL_KDD 데이터에 대해서 설명한다. 3장에서는 데이터 전처리 방법을 설명하고 4장에서는 탐지율과 실시간성 모두를 보장하는 유전자 알고리즘 기반의 특징 추출 방법을 제시한다. 5장에서는 인공신경망을 사용한 침입탐지 시스템을 설계하고 6장에서 기존에 제시된 방법들과 성능을 비교한다. 그리고 7장에서 결론을 내린다.

2. NSL_KDD 데이터

제안하는 시스템의 구현 및 성능평가에 사용한 데이터는 KDD'99 데이터[7]의 수정 버전인 NSL_KDD 데이터[8]이다. KDD'99 데이터는 MIT 링컨 연구소가 DARPA 침입탐지 평가 프로그램을 수행하면서 만들어진 데이터 집합이다. 9주간에 걸쳐 미 공군의 지역 네트워크(LAN)을 모사하고 38가지의 공격 방법을 사용하여 얻은 것으로 이후 침입탐지 경진 대회에 사용되었다. 이후 KDD'99 데이터는 침입탐지 시스템의 설계 및 성능 평가에 지속적으로 사용되어 왔다.

KDD'99 데이터는 약 500만개의 훈련 데이터와 30만개의 평가 데이터로 구성되어 있다. 훈련 데이터의 경우 정상과 24가지의 공격이 있는 반면 평가 데이터에는 24가지 이외에 추가로 14가지 공격이 포함되어 있다. 공격의 종류는 <표 1>과 같이 4가지 카테고리로 범주화 할 수 있다.

하지만, KDD'99 데이터는 데이터의 규모가 지나치게 크고 중복된 데이터가 있는 등 가공하지 않은 상태 그대로 사용하는데 많은 문제점이 있다. 이러한 이유로 데이터의 일부만을 자의적으로 선별해 연구에 사용하는 경향이 있어왔다. 하지만 자의적 데이터 사용은 연구 결과의 객관성을 떨어뜨리는 한편 비교되는 방법들 간의 공정한 비교를 어렵게 하였다. 이를 해결하기 위해 M. Tavallaee 등[9]에 의해 NSL_KDD 데이터가 제안되었다. NSL_KDD 데이터는 KDD'99 데이터의 부분 집합이긴 하지만 KDD'99 데이터를 면밀히 분석한 후 데이터의 중복성을 제거하고 공격 유형에 따라 적정한 수의 데이터를 배분함으로써 NSL_KDD 데이터를 사용한 연구 결과에 대해 신뢰성과 공정성을 확보할 수 있게 하였다. 최근 많은 연구들이 KDD'99를 사용하기 보다 NSL_KDD 데이터를 즐겨 사용하고 있는 추세이다.

<표 1> KDD'99 데이터에 포함된 4가지 공격 유형

공격 유형	설명
DOS	서비스 거부 공격, (ex: syn flood)
R2L	원격으로부터의 비인가된 접속 (ex: 패스워드 추정)
U2R	루트 권한 획득을 위한 비인가 접근 (ex: 버퍼 오버플로우 공격)
Probing	프로빙 공격 (ex: 포트 스캐닝)

하지만, KDD'99 데이터는 데이터의 규모가 지나치게 크고 중복된 데이터가 있는 등 가공하지 않은 상태 그대로 사용하는데 많은 문제점이 있다. 이러한 이유로 데이터의 일부만을 자의적으로 선별해 연구에 사용하는 경향이 있어왔다. 하지만 자의적 데이터 사용은 연구 결과의 객관성을 떨어뜨리는 한편 비교되는 방법들 간의 공정한 비교를 어렵게 하였다. 이를 해결하기 위해 M. Tavallaee 등[9]에 의해 NSL_KDD 데이터가 제안되었다. NSL_KDD 데이터는 KDD'99 데이터의 부분 집합이긴 하지만 KDD'99 데이터를 면밀히 분석한 후 데이터의 중복성을 제거하고 공격 유형에 따라 적정한 수의 데이터를 배분함으로써 NSL_KDD 데이터를 사용한 연구 결과에 대해 신뢰성과 공정성을 확보할 수 있게 하였다. 최근 많은 연구들이 KDD'99를 사용하기 보다 NSL_KDD 데이터를 즐겨 사용하고 있는 추세이다.

NSL_KDD 데이터도 KDD'99 데이터와 마찬가지로

4지 공격 유형으로 구성되어 있으며 각 레코드는 41개의 특징들로 구성되어 있다.

한편, NSL_KDD 데이터에 있는 서비스 거부 공격은 <표 2>와 같이 6가지 종류로 되어 있으며 그 레코드 수도 표에서 확인할 수 있다. 정상 레코드와 서비스 거부 공격 레코드 사이에 양적 차이가 있으며 공격 유형에도 많은 편차가 있음을 알 수 있다.

<표 2> NSL_KDD 데이터에 있는 6가지 공격 유형과 레코드 수 구성

	Normal	Neptune	Teardrop	Smurf	Pod	Back	Land
Training data	67344	41214	892	2646	201	956	18
Test data	9711	4657	12	665	41	359	7

3. 데이터 전처리

특징들을 인공신경망과 같은 학습 기계의 입력으로 사용하기 위해서는 특징들이 모두 수치화 되어있어야 한다. 하지만 NSL_KDD 데이터에 있는 특징 중에는 protocol_type과 같이 심볼릭 특징이 있어 이를 수치화 해야할 필요가 있다. 또한 src_bytes나 dst_bytes처럼 10억이 넘는 값을 가지고 있어 다른 특징들에 대해 치우침(bias) 현상을 유발하는 특징들도 있어 적당한 범주내의 값으로의 정규화가 필요하다. 정규화 방식으로는 T. Naidoo[10]가 제시한 방법과 M. Sabhanani[11]가 제시한 방법 등이 있는데, 본 논문은 M. Sabhanani가 제시한 방법을 사용한다. 정규화는 특징의 유형에 따라 4가지로 나누고 각 유형에 따라 다음과 같이 정규화 한다.

우선 protocol_type과 같이 값이 심볼인 특징은 값의 종류에 따라 0부터 양의 정수를 부여하는 방식을 사용한다. 예를 들어 tcp, udp, icmp로 구성되어 있는 protocol_type의 경우 tcp는 0, udp는 1, icmp는 2를 각각 부여한다. scr_bypes나 dst_bytes처럼 비록 그 값이 수이지만 다른 특징에 비해 아주 커서 인공신경망에 사용하는 경우 치우침을 일으키는 특징은 10을 베이스로 한 로그값을 사용한다. 마지막으로 이렇게 수치화된 각 특징들을 모두 0과 1사이 값으로 선형 정규화 한다.

4. 특징 추출 방법 : 다목적 유전자 알고리즘

6가지 서비스 공격에 대해 높은 탐지율과 작은 탐색시간이라는 두 가지 상충되는 목적을 보장하는 특징 집합을 추출하고자 다목적 유전자 알고리즘[12]을 제시한다. 다중 목적 유전자 알고리즘은 여러 가지 상충관계에 있는 목적들을 대상으로 최적해를 찾기 위해 사용하는 잘 알려진 메타 휴리스틱 알고리즘 중 하나이다.

최적 특징 집합을 추출하는 문제는 주어진 특징 집합 F에 대해 비용함수 C가 $C.f \rightarrow v\,(0 \leq v)$와 같을 때 v값을 최소로 하는 특징 조합 f을 추출하는 문제로 정의할 수 있다.

4.1 해의 표현

41가지 특징으로 구성된 특징 집합에서 주어진 비용함수를 최소화하기 위한 특징 조합은 조합에 특징이 포함되는지의 여부에 따라 0, 1을 부여한 다음과 같은 41차원의 벡터로 표현할 수 있다.

$S = <s_1, s_2, s_3, ..., s_i, ..., s_{41}>,\ s_i \in \{0, 1\}$

예를 들어 모든 특징이 사용되는 특징 조합을 대표하는 해는 모든 요소 값이 1을 갖는 41차원의 벡터 <1, 1, 1, ..., 1>로 표현된다. 따라서 41가지의 특징으로 구성할 수 있는 특징 조합의 총수는 2^{41}-1 가지가 된다.

4.2 적합 함수

선택할 특징 조합의 목적은 두 가지이다. 우선 서비스 거부 공격에 대한 탐지율을 최대화하는 것이다. 다른 목적은 서비스 거부 공격의 유무 및 종류를 최대한 빨리 탐지해서 관리자에게 알려 주는 것이다. 공격 탐지 시간과 밀접하게 연관되어 있는 중요한 요소 중 하나는 특징 벡터에 포함된 특징의 수이다. 특징의 수가 작을수록 특징 값을 확정하고 이를 이용해 공격 유무 및 종류를 알아내는데 걸리는 시간이 작다. 따라서 특징 조합(벡터)이 갖추어야할 바람직한 속성은 높

은 탐지율을 보장하면서 그 수가 작아야 한다. 하지만 특징 수의 크기와 탐지율과는 일반적으로 양의 상관관계를 가지므로 특징의 수가 작으면서 높은 탐지율을 보장하기는 쉽지 않다.

두 가지 상충하는 목적을 달성하기 위해 사용하는 목적함수의 구성 방법에는 여러 가지가 있지만 본 논문에서는 두 가지 목적에 대한 함수를 별도로 정의한 다음 이들의 가중치 합 방식을 제안한다. 우선 탐지율 보장을 위한 목적함수를 설명한다.

앞에서도 언급했지만 특정 목적 달성을 위한 특징 조합 선택 방법에는 래퍼방식과 필터방식이 있는데, 특징 조합의 창발적 특성을 보장할 수 있는 방법은 래퍼방식이다. 하지만 래퍼방식의 단점인 장시간의 학습시간과 특정 기계학습 방식에 과적응문제가 발생할 수 있다. 이를 피하기 위해 주어진 특징 벡터의 적합성 평가를 위해 k-평균 클러스터링을 이용하는 방법이 제안되었는데[13,14], 논문도 이 방법을 사용한다. k-평균 클러스터링을 이용하는 방법은 다음과 같다. 우선 주어진 특징 벡터 S를 이용해 데이터 집합을 대상으로 k-평균 클러스터링을 실행한 후 그 결과로 얻어진 각 데이터 x의 소속값 $p(x)$와 원 소속값 $q(x)$를 비교하여 식(1)과 같이 $\omega(x)$를 구한다.

$$\omega(x)=\begin{cases}1 & \text{if } p(x)=q(x)\\ 0 & otherwise\end{cases} \tag{1}$$

주어진 특징 조합 S에 대한 탐지율 측면에서의 적합성은 식(2)와 같이 모든 데이터에 대해 $\omega(x)$를 구하고 이를 합한 후 전체 데이터 수로 나눈 비율로 정의된다.

$$Fit_{detect}(S)=\sum_{i=1}^{N}\omega(x_i)/N \tag{2}$$

여기서 N은 데이터의 크기를 나타낸다. 한편, 특징 조합의 실시간성과 관련이 있는 벡터 크기에 대한 목적 함수는 식(3)과 같이 특징 벡터의 크기에 비례하도록 정의한다.

$$Fit_{len}(S)=(FN-\phi(S))/FN \tag{3}$$

여기서 FN은 전체 특징의 개수를 나타내므로 41이다. $\phi(S)$는 주어진 해 S에서 1값, 즉 선택된 특징의 개수를 말한다.

마지막으로 주어진 특징 조합(해) S에 대한 탐지율과 실시간성을 모두를 목적으로 하는 적합함수는 앞에서 정의된 두 목적함수 식(2)와 식(3)의 가중치 합으로 정의된다.

$$Fit(S)=\lambda Fit_{detect}(S)+(1-\lambda)Fit_{time}(S),\quad 0\le\lambda\le 1 \tag{4}$$

λ는 두 목적 함수의 가중치를 나타내는 매개변수 값으로 두 목적의 중요성에 따라 적절히 선택해 사용할 수 있다.

4.3 유전자 알고리즘

다양한 목적함수의 가중치 합을 적합함수로 사용하는 유전자 알고리즘의 절차는 하나의 목적함수를 적합함수로 사용하는 일반적인 유전자 알고리즘의 절차와 큰 차이가 없다. 실제 사용한 매개변수를 이용해 알고리즘을 설명하면 다음과 같다.

단계 1. 초기 해집합 생성
초기 해집합을 구성하기 위해 임의로 선택된 41차원의 이진 벡터 100개를 생성하고 수식(4)를 이용해 각 해에 대한 적합함수 값을 계산한다.

단계 2. 선택(Selection) 연산
새로운 해집합을 생성하기 위해서는 이전 해집합으로부터 좋은 부모해를 선택해야 한다. 유전자 알고리즘에서 사용하는 선택 연산에는 다양한 종류가 제안되어 있는데, 본 논문에서는 룰렛 휠 선택 연산으로 알려진 적합함수 값에 비례해 두 개의 해를 선택하는 방식을 사용하였다. 다만, 빠른 수렴을 위해 엘리티즘을 사용하였다. 즉, 이전 해집합에서 적합함수 값이 10% 이내에 드는 해는 별도의 교차연산 없이 다음 해집합에 그대로 추가하였다.

단계 3. 교차(Crossover) 연산
적합함수 값에 비례하게 두 개의 해를 선택한 후 두

해에 대해 교차연산을 적용하여 새로운 두 개의 해를 생성한다. 이 때 교차연산은 한 점 교차연산(Single Point Crossover) 방식을 사용하였다. 한 점 교차연산이란 해안의 임의의 점을 선택하고 점을 중심으로 앞과 뒤로 분리한 후 두 개의 해로부터 교차 연결해 새로운 해 두 개를 생성하는 방식을 말한다.

단계 4. 돌연변이(Mutation) 연산
돌연변이율에 대한 완벽한 지침은 없으나 일반적으로 너무 크지 않게 주는 것이 해의 수렴성을 보장한다. 본 논문에서는 다양한 돌연변이율을 가지고 실험 후에 1%를 돌연변이율로 사용해 특징조합의 요소를 선택한 후 값이 0이면 1로, 1이면 0으로 변형하여 해공간의 다양성을 보장하였다.

단계 5. 종료 조건
새로 생성된 해집합의 모든 해들에 대해 적합함수 값을 구하고 100회의 해집합 생성이 행해졌으면 알고리즘을 종료한다. 그렇지 않은 경우엔 단계 2로 이동해 동일한 절차를 반복한다.

유전자 알고리즘이 종료하면 100회 반복에서 얻어진 해 중 최고의 적합함수 값을 가진 해의 특징 조합을 최적 특징 조합으로 사용한다.

5. 인공신경망 기반 침입탐지

특징 조합 추출이 완료되었으면 실제 침입 여부 및 종류를 판별할 침입 탐지 시스템을 구현해야 한다. 본 논문은 인공신경망 기반의 침입 탐지 시스템을 구현하였다. NSL_KDD 데이터를 이용해 다양한 기계학습 방법을 이용해 탐지율을 비교한 실험[14]에서 인공신경망은 높은 성능을 보여 주었다. 본 논문도 제안한 다목적 특징 조합을 이용한 침입 탐지 시스템을 구현하기 위해 인공신경망을 사용하였다.

우선 제안한 특징 선택 알고리즘을 이용해 얻은 특징 조합만을 이용해 NSL_KDD 데이터를 새롭게 가공하여 데이터 집합을 생성하였다. 사용한 인공신경망은 일반적으로 사용되는 3계층(입력층, 은닉층, 출력층)의 구조를 가진 다층 퍼셉트론형태이다. 입력 노드의 개수는 특징 조합에서 사용되는 특징들의 개수와 같고 출력 노드의 개수는 6가지 서비스 거부 공격과 정상 레코드를 대표하기 위해 7개의 노드로 구성하였다. 은닉 계층에 사용된 노드의 개수는 다양한 실험을 통해 가장 높은 성능을 보여준 개수를 선택하여 사용하였다. 학습을 위해 출력층에 할당한 목표값은 해당 클래스에 대해서는 0.9 값을 부여하고 나머지 클래스는 0.1 값을 부여하였다. 예를 들어 정상 레코드에 대한 목적 출력값은 <0.9, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1>을 부여한다. 서비스 거부 공격들은 해당하는 출력 노드에 0.9 값을 부여하여 학습을 유도하였다. 학습 알고리즘은 오류 역전파 알고리즘을 사용하였으며 다양한 학습률과 모멘텀 값을 사용해 실험한 후 가장 좋은 성능을 보여준 값들을 선정하여 최종 실험에 사용하였다.

입력층을 제외한 모든 노드는 시그모이드 함수 $n(w)=(1+e^{-w})^{-1}$를 사용하였고, 훈련집합 전체를 대상으로 학습을 한 후 시스템의 탐지율이 이전 학습 후의 탐지율에 비해 0.1% 이상의 개선이 이루어지지 않으면 학습을 종료하였다.

6. 실험 및 성능 비교

<표 2>에 제시된 7가지 종류로 구성된 학습 데이터를 이용해 인공신경망을 학습 시킨 후 테스트 데이터를 이용해 탐지율을 조사하였다. 또한 학습에 걸린 시간과 테스트에 걸린 시간을 실험하였다.

[14]에는 본 논문과 동일한 데이터를 이용해 지역탐색(local search) 알고리즘과 시뮬레이티드 어닐링 알고리즘 사용해 얻은 결과가 제시되어 있어서 이들 결과와 비교분석하였다. <표 3>에 나타난 다목적 유전자 알고리즘의 결과는 특징 조합 선택을 위해 사용한 적합함수의 가중치 λ를 0.5로 설정해 얻은 결과이다. 표 3에서 알 수 있듯이 탐지율(accuracy)은 특징 벡터의 크기를 명시적인 목적으로 사용하지 않은 경우에 비해 약간 낮지만 무시할만한 수준이다. 이에 반해 특징 벡터의 크기 및 학습시간, 테스트 시간에서는 확연한 성능 개선을 보여준다. 실제 트래픽이 많은 네트워크에서의 이상 징후를 실시간에 정확하게 탐지하기 위해서는 작은 테스트 시간에 대한 요구가 필수적이라는 사실에서 이는 중요한 개선이라고 할 수 있다.

<표 3> 성능 비교

	accuracy (%)	number of features	time for training (sec)	time for testing (sec)
all features	96.98	41	799.65	1.48
Local search	96.77	19.05	315.99	0.71
Simulated annealing	96.83	18.00	296.79	0.64
M-Obj GA	96.32	15.6	271.1	0.57

7. 결 론

본 논문은 인공신경망 기반의 이상 징후 탐지 시스템을 위한 특징 조합 선택 방법을 제안하였다. 제안 방법은 높은 탐지율과 적은 탐지시간이라는 상충관계에 있는 두 가지 목적 모두를 만족하기 위해, 각 목적에 대한 함수를 정의 하고 목적 함수간의 가중치 합을 적합 함수로 사용하는 다목적 유전자 알고리즘에 기반하고 있다. NSL_KDD 데이터를 이용해 실험하고 기존에 제시된 탐지율만을 목적으로 한 다른 방법들과 비교했을 때 비록 탐지율에서는 무시할만한 수준의 성능차를 보여준 반면 사용하는 특징 수나 훈련, 테스트에 걸리는 시간은 상대적으로 높은 성능을 보여줬다.

본 논문은 기계학습 기반의 이상 징후 탐지 시스템을 위한 특징 조합 선택 방법들이 높은 탐지율 만을 강조함에 반해 빠른 탐지를 명시적으로 목적함수에 고려하여 기존의 단점을 극복하기 위해 다목적 탐색 알고리즘을 제시했다는 점에서 의미가 있다. 하지만, 상충하는 목적들을 동시에 만족하는 파레토 최적해들을 얻기 위한 다른 방법들에 대한 연구 및 각 특징들을 대상으로 값을 결정하는데 드는 시간이 다르다는 점 등을 고려해서 보다 정확한 설계 및 실험이 필요하다. 앞으로 다양한 관점을 도입하여 보다 나은 결과물이 나올 수 있도록 방법 및 실험을 확대할 계획이다.

참고문헌

[1] G. Wang, J. Hao, J. Ma, and L. Huang, “A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering”, Expert Systems with Applications, Vol. 37, Issue 9, pp. 6225 - 6232, 2010.

[2] Md. Al mohediHasan, M. Nasser, and B. Pal, “On the KDD’99 Dataset: Support Vector Machine Based Intrusion Detection System (IDS) with Different Kernels”, International Journal of Electronics Communication and Computer Engineering, Vol. 4, Issue 4, pp. 1164-1170, 2013.

[3] H. S. Huang, “Supervised feature selection: A tutorial”, Artificial Intelligence Research, Vol. 4, No. 2, 2015.

[4] H. G. Kayacik, A. N. Zincir-Heywood, and M. I. Heywood, “Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets,” in Thrid Annual Conference on Privacy, Security and Trust, St. Andrews, New Brunswick, Canada, 2005.

[5] A. A. Olusola, A. S. Oladele, and D. O. Abosede, “Analysis of KDD ’99 Intrusion Detection Dataset for Selection of Relevance Features,” in Proc. of the World Congress on Engineering and Computer Science, Vol. 1, 2010.

[6] S. Parazad, E. Saboori, and A. Allahyar, “Fast Feature Reduction in Intrusion Detection Datasets,” in MIPRO, Proceedings of the 35th International Convention, pp.1023-1029, 2012.

[7] KDD Cup 1999. Available on:http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, 2007.

[8] NSL_KDD data set. Avalilable on: http://nsl.cs.unb.ca/NSL-KDD/

[9] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, “A Detailed Analysis of the KDD CUP 99 Data Set,” Proc. 2009 IEEE Int. Conf. Comput.

Intell. Security Defense Appl. CISDA, pp. 53-58, 2009.

[10] T. Naidoo, J. R. Tapamo and A. McDonald, “Feature selection for anomaly‐based network intrusion detection using cluster validity indices”, In: SATNAC: Africa - The Future Communications Galaxy, 2015.

[11] M. Sabhnani and G. Serpen, “Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context,” Proc. of International Conference on Machine Learning: Models, Technologies, and Applications, pp. 209-215, 2013.

[12] A. Konak, D. Coit, and A. Smith, “Multi-objective optimization using genetic algorithms: a tutorial”, Reliability Engineering & System Safety in Special Issue - Genetic Algorithms and Reliability, vol. 92, pp. 992‐1007, 2006.

[13] S. H. Kang, and K. J. Kim, “A feature selection approach to find optimal feature subsets for the network intrusion detection system”, Cluster Computing, Vol. 19, Issue 1, pp 325‐333, 2016.

[14] I. S. Jeong, H. K. Kim, T. H. Kim, D. H. Lee, K. J. Kim and S. H. Kang, “A Feature Selection Approach Based on Simulated Annealing for Detecting Various Denial of Service Attacks“, Convergence Security, Vol. 1, pp. 1‐18., 2016.

[저 자 소 개]

김 태 희(Tae-Hee Kim)

1991년 2월 : 동신대학교 전자계산학과 (공학사)
1993년 2월 : 전남대학교 전산통계학과 (이학석사)
1999년 2월 : 전남대학교 전산통계학과 (이학박사)
1998년 2월 ~ 현재 : 동신대학교 융합정보보안전공 교수
<관심분야> : 정보공학, 데이터베이스 보안, 네트워크보안
email : thkim@dsu.ac.kr

강 승 호 (Seung-Ho Kang)

1994년 8월 : 전남대학교 전산학과 학사
2003년 2월 : 전남대학교 전산학과 석사
2009년 8월 : 전남대학교 전산학과 박사
2010년 10월 : 국가수리과학연구소 연구원
2013년 9월 ~ 현재 : 동신대학교 융합정보보안전공 교수
<관심분야> : 네트워크보안, 알고리즘, 지능형시스템
email : drminor@dsu.ac.kr