https://doi.org/10.14400/JDC.2017.15.6.391

퍼지와 인공 신경망을 이용한 침입탐지시스템의 탐지 성능 비교 연구

양은목*, 이학재**, 서창호***
숭실대학교 소프트웨어학부*, 전남대학교 전자컴퓨터공학과**, 공주대 응용수학과***

Comparison of Detection Performance of Intrusion Detection System Using Fuzzy and Artificial Neural Network

Eun-Mok Yang*, Hak-Jae Lee, Chang-Ho Seo*****
School of Software, Soongsil University*
Dept. of Electronics and Computer Engineering, Chonnam National University**
Dept. of Applied Mathematics, Kongju National University***

요 약 본 논문에서는 “퍼지 컨트롤 언어를 이용한 공격 특징 선택기반 네트워크 침입탐지 시스템”[1]과 “RNN을 이용한 공격 분류를 위한 지능형 침입탐지 시스템 모델”[2]의 성능을 비교 하였다. 이 논문에서는 KDD CUP 99 데이터 셋[3]을 이용하여 두 기법의 침입 탐지 성능을 비교하였다. KDD CUP 99 데이터 셋에는 훈련을 위한 데이터 셋과 훈련을 통해 기존의 침입을 탐지 할 수 있는 테스트 데이터 셋이 있다. 또한 훈련 데이터 및 테스트 데이터에 존재 하지 않는 침입의 유형을 탐지할 수 있는가를 테스트 할 수 있는 데이터도 존재한다. 훈련 및 테스트 데이터에서 좋은 침입탐지 성능을 보이는 두 개의 논문을 비교하였다. 비교한 결과 존재하는 침입을 탐지 하는 성능은 우수하지만 기존에 존재하지 않는 침입을 탐지 하는 성능은 부족한 부분이 있다. 공격 유형 중 DoS, Probe, R2L는 퍼지를 이용하는 것이 탐지율이 높았고, U2L은 RNN을 이용하는 것이 탐지율이 높았다.

주제어 : 침입탐지, 퍼지, 신경망, RNN, KDD CUP 1999 dataset

Abstract In this paper, we compared the performance of "Network Intrusion Detection System based on attack feature selection using fuzzy control language"[1] and "Intelligent Intrusion Detection System Model for attack classification using RNN"[2]. In this paper, we compare the intrusion detection performance of two techniques using KDD CUP 99 dataset. The KDD 99 dataset contains data sets for training and test data sets that can detect existing intrusions through training. There are also data that can test whether training data and the types of intrusions that are not present in the test data can be detected. We compared two papers showing good intrusion detection performance in training and test data. In the comparative paper, there is a lack of performance to detect intrusions that exist but have no existing intrusion detection capability. Among the attack types, DoS, Probe, and R2L have high detection rate using fuzzy and U2L has a high detection rate using RNN.

Key Words : Intrusion Detection, Fuzzy, Neural Network, RNN, KDD CUP 1999 dataset

* This research was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government(MISP)(2016R1A4A1011761).
Received 14 April 2017, Revised 10 May 2017
Accepted 20 June 2017, Published 28 June 2017
Corresponding Author: Change-Ho Seo(Department of Applied Mathematics Kongju National University)
Email: chseo@kongju.ac.kr
ISSN: 1738-1916

1. 소개

네트워크 기술의 발전과 침입 기술이 고도로 발달되면서 네트워크를 통해 발생되는 위협은 날로 증가되고 있지만 다양한 침입을 탐지하지 못하고 있다. 네트워크를 통해 개인 IT기기 등에 저장되어 있는 개인정보, 회사 및 국가 기밀 등 민감한 정보들이 위협하고 있다.

이들 위협으로부터 대응하기 위해 침입탐지 시스템에 관한 연구로 KDD CUP 1999 데이터 셋이 발표되고 이 데이터 셋과 인공지능을 이용한 다양한 연구들이 많이 진행되고 있다.

침입탐지시스템을 분류하는 방법은 데이터소스 기반, 분석기법 기반, 경과 시간 기반, 제어 전략 기반, 대응 옵션 기반으로 분류할 수 있다.

데이터소스 기반으로는 호스트 기반, 네트워크 기반, 애플리케이션 기반으로 분류할 수 있고, 분석기법 기반으로는 오용탐지 및 비정상행위 탐지로 분류할 수 있다. 또한 경과시간 기반으로는 실시간 탐지 및 비실시간으로 분류하고, 제어 전략 기반으로는 중앙 집중 기반, 부분분산 기반 및 완전분산 기반으로 분류한다. 마지막으로 대응 옵션으로는 적극적 대응과 소극적 대응으로 분류한다.

침입탐지 알고리즘은 패턴 기반, 인공 신경망, 퍼지, 규칙 기반, SVM, 유전자 알고리즘, 의사 결정 트리, 기타 통계 적인 방법 등 다양한 방법으로 연구되었다[4].

본 논문에서는 KDD CUP 99 데이터 셋을 이용하여 침입탐지 성능을 평가한 논문 중에 성능이 우수한 두 개의 논문을 비교 연구 하였다. 전반적인 논문의 구성은 2장에서 비교논문에 사용된 인공지능 기법에 대하여 소개하고 3장은 KDD CUP 99 데이터 셋의 구성에 대해 소개하고 4장에서는 “퍼지 컨트롤 언어를 이용한 공격 특징 선택기반 네트워크 침입탐지 시스템”[1]와 “RNN을 이용한 공격 분류를 위한 지능형 침입탐지 시스템 모델” [2]의 탐지 방법을 비교한다. 그리고 5장에서는 탐지 성능을 비교하고 장・단점을 분석한다.

2. 인공지능

2.1 퍼지

퍼지는 애매함 문제에 대해 의사결정, 문제해결, 제재 등을 요청할 경우 이론으로부터 정보를 검색, 인식, 고찰, 판단하는 순으로 지적 처리 모델을 제공하는 것을 목표로 한다. 본 논문의 비교 대상논문에서는 퍼지의 표현을 침입정도가 매우 낮음, 낮음, 보통, 높음, 매우 높음의 5단계로 표현하고 있다[1].

임의의 집합 X에 있어서 퍼지집합 A란 맴버십 함수($\mu_A(x)$)에 의해 특징이 주어진 집합이다. x가 퍼지 집합 A에 속하는 정도 또는 그레이드를 나타내는 정도를 맴버십 함수라고 하는데 1에 가까우면 속하는 정도가 높은 것이고 0에 가까우면 속하는 정도가 낮다는 것이다.

멥버십 함수는 형태에 따라 정규형은 맴버십 함수 값이 1이 되는 a 퍼지수의 중심에서 양쪽으로 멀어짐에 따라 작아지는 것이고, 삼각형은 가장 많이 쓰이고 간단한 맴버십 함수로 삼각형 퍼지수=(a_1, a_2, a_3)이다. 또한 퍼지수를 구성하는 좌우의 부분이 다른 형의 함수를 L-R 퍼지수라고 하고 오른쪽으로 올라가는 함수를 좌측함수, 오른쪽으로 내려가는 함수를 우측함수라 한다. 사다리꼴 맴버십 함수는 4점으로 (a, b, c, d)로 나타낸다. 마지막으로 지수형 맴버십 함수가 있다[5].

맴버십 함수를 결정하는 일반적인 방법 및 표준적인 맴버십 함수라는 것도 없다. 맴버십 그레이드는 무엇에 대한 비율을 나타내는 것이 아니므로 확률이 아니다. 맴버십 그레이드는 일정부분 개인의 주관에 의하여 결정된다. 맴버십 함수를 정하는데 대상 x가 그 개념에 속하는 정도가 높으면 맴버십 값도 커지고, 낮으면 맵버십 값도 낮아진다. 이와 같이 맴버십 함수는 대소의 순서관계를 반영하여 맴버십 함수의 값을 정하는 것이 중요하다.

맴버십 함수를 추정하는 방법 평균법과 위치 파라메터 추정법이 있는데 평균법의 그레이드는 객관적 그레이드와 주관적 그레이드의 합으로 나타내어 지는데 만약 주관적인 그레이드의 평균이 0이면 객관적 그레이드는 n명의 평가자의 주관적인 맴버십 그레이드의 평균으로 구해진다. 이는 평가자가 많을수록 삼각형 함수나 사다리꼴 함수가 곡선에 가까워져 최초의 각 개인의 맴버십 함수의 모양과 달라지는 문제점이 있다. 위치 파라메터 추정법은 평균법의 문제점이 맴버십 함수의 모양이 달라지지 않는다. 위치 파라메터 추정법은 주관적 그레이드의 오차를 인정하고 평가자의 모든 오차의 제곱합을 최소로 하는 방정식을 통해 새로운 맴버십 함수를 구한다.

맴버십 함수를 구하는 것은 실제보다 더 어려울 수도 있다. 하지만 맴버십 함수가 정해지면 퍼지 집합은 정확하게 정의 내릴 수 있다. 퍼지수의 기본 연산에는 합집합, 교집합, 여집합에 최대, 최소(max,min) 계산에 퍼지 논리가 쓰인다. 합집합은 max, 교집합은 min, 여집합은 $1-\mu_A(x)$로 계산한다[6].

2.2 신경망

RNN(Recurrent Neural Network)은 음악, 음성, 동영상, 문자열 등 순차적인 정보가 담긴 데이터 학습에 널리 쓰인다. 기존의 인공신경망은 입력, 히든, 출력 레이어로 단순히 각 층의 뉴런이 연결된 구조라면 RNN은 순환 가중치(Recurrent Weight)는 히든 레이어에 추가된 구조이다. 순환 가중치는 과거의 데이터에 대한 정보를 기억할 수 있는 기능이 있다. 이와 같은 기능은 새로운 데이터를 처리할 때 과거의 데이터에 대한 정보를 사용할 수 있다[5]. 그래서 우리가 현재의 내용을 파악할 때 과거의 기억을 사용하듯이 RNN도 순차적이 데이터 속에서 과거의 정보를 사용하여 현재의 내용을 파악할 수 있도록 한 신경망기법이다. RNN의 학습은 기존 인공신경망의 학습알고리즘 오류역전파(Error Back Propagation)를 확장한 시간에 따른 역전파(Back Propagation Through Time) 알고리즘을 통해 학습한다[7].

3. KDD CUP 99 데이터 셋

인공지능을 이용한 침입탐지 시스템에 관한 연구에서 성능을 평가하고자 할 때는 크게 두 가지 방법이 있다. 첫 번째는 자체 데이터를 수집하여 평가하는 방법과 두 번째는 KDD CUP 99 데이터 셋[3]을 사용하여 평가하는 방법이다. 두 번째의 방법이 좀 더 많이 사용되어 지는데 그 이유는 KDD CUP 99 데이터 셋은 네트워크 트래픽을 정상 또는 공격유형 포함하고 있기 때문에 학습을 수행하여 나온 결과와 비교할 수 있기 때문이다.

KDD 훈련 데이터는 41개의 특징을 포함하고 정상 또는 하나의 공격유형으로 표시된다. 공격유형은 다음의 4개의 유형이다[8].

- Denial of Service Attack(DoS) : DoS 공격은 공격 대상의 시스템에 메모리를 포함한 리소스를 많이 사용하게 하여 정상적인 서비스 요청을 거부하게 하는 공격이다.
- User to Root Attack(U2R) : U2R 공격은 일반 사용자 계정으로 로그인 후 스니핑, 암호 사전공격 등의 공격으로 승인 받지 않은 루트 권한을 획득하는 공격이다.
- Remote to Local Attack(R2L) : R2L 공격은 원격지에서 네트워크를 통해 패킷을 보낼 수는 있지만 공격 시스템에 계정이 없는 공격자가 해당 시스템의 로컬 엑세스를 획득하기 위v 한 공격이다.
- Probing Attack: Probing은 보안 컨트롤을 우회할 목적으로 컴퓨터 네트워크에 대한 정보를 수집하기 위한 시도이다.

KDD CUP 99 데이터 셋의 특징은 다음의 세 가지 그룹으로 분류할 수 있다.

- 기본 특징 : TCP/IP 연결에서 추출할 수 있는 모든 속성을 포함한다. 이것은 탐지 지연을 발생 시킬 수 있다.
- 트래픽 특징 : 시간 기반으로 추출하는 데이터의 속성을 포함한다. 이러한 특징은 두 개의 그룹으로 분류할 수 있다. 첫 번째는 동일 호스트 특징이고 현재 연결과 같은 동일 호스트의 프로토콜 동작, 서비스 등 관련 통계들을 계산하여 2초 이내의 연결 인지를 조사한다. 두 번째는 동일 서비스 특징으로 현재 연결과 같은 서비스인지를 2초만 연결하아 조사한다. 트래픽 특징은 포스트 켄 등 2초 시간으로 침입 패턴을 생성하지 않으므로 동일 호스트 및 동일 서비스 특징은 2초의 시간보다 100개의 연결 기반으로 다시 계산되어 졌다.
- 콘텐츠 특징 : R2L 및 U2L 공격은 DoS 및 Probing 공격과 달리 침입에서 반복되는 패턴이 없고 패킷 데이터 부분에 포함되며 단일 연결로 이루어져 있다. 이러한 공격을 탐지하기 위해서는 데이터 부분에서 실패한 로그인 횟수 등 찾을 수 있는 몇 가지 특징이 필요한데 이것이 콘텐츠 특징이다.

학습데이터에는 24가지 공격유형이 존재하고 테스트 데이터에는 추가로 14가지 공격유형이 존재한다. KDD CUP 1999 데이터 셋에는 훈련 데이터 kddcup.data.gz, 성능을 측정할 수 있는 테스트 데이터 kddcup.data 10 percent.gz, 침입 유형이 표시 되어 있지 않은 데이터가

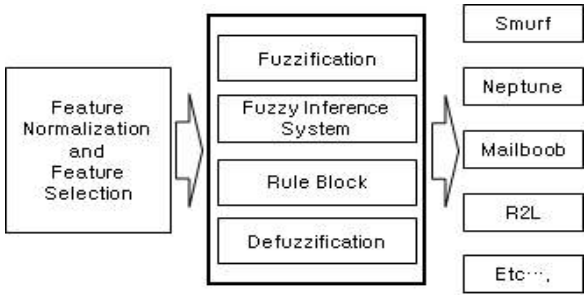
있다. 또한, 연구자들은 새로운 공격 유형은 기존의 것을 활용하여 새로운 공격 한다고 생각하기 때문에 기존의 침입 유형과 새로운 침입 유형이 존재하는 데이터 corrected.gz가 있다.

4. 침입탐지시스템의 탐지 방법 비교

4.1 퍼지

"퍼지 컨트롤 언어를 이용한 공격 특징 선택기반 네트워크 침입탐지 시스템"[1]에서는 KDD CUP 99 데이터 셋에서 특징을 추출해서 선택하고 계층화된 퍼지 제어 언어를 제안하였다.

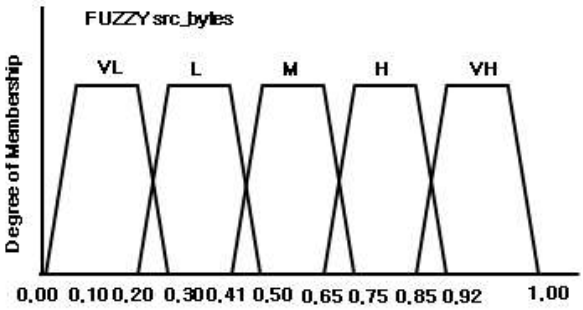
데이터 셋에서 특징을 추출을 위한 첫 번째 과정은 서로 다른 공격유형을 분류하기 위해서 다양한 공격 유형 중에 동일한 공격유형의 부분집합을 선택한다. 이것은 퍼지 기반 계층 분류이다. 두 번째는 연속 값을 갖는 변수는 값의 범위(0-6,291,668)에서 큰 차이가 있기 때문에 최대-최소 방법으로 [0,1]의 값으로 정규화를 한다. 세 번째는 엔트로피 기준으로 클래스 간 엔트로피 값이 매우 높고 클래스 내 엔트로피가 매우 낮으면 퍼지 입력에서 제외하였다. 그래서 41개의 특징 중 3개의 범주형 변수와 22개의 연속형 변수를 사용하여 침입을 분류하였다.



[Fig. 1] Architecture of Layered Fuzzy Control Language

계층적 퍼지 제어 언어는 퍼지화 전에 특징을 일반화하고 선택하였다. 첫 번째로 퍼지화는 맴버십 함수를 정의하고, 두 번째로 퍼지추론 시스템은 퍼지 규칙 기반으로 공격 유형을 탐지한다. 마지막으로 디퍼지화는 계층적 분류자를 사용하여 특정 공격을 크리스프 값으로 변환한다.

맴버십 함수는 다양한 맴버십 함수가 있는데 KDD 데이터 셋에 적합한 사다리꼴 맴버십 함수를 사용하였다.



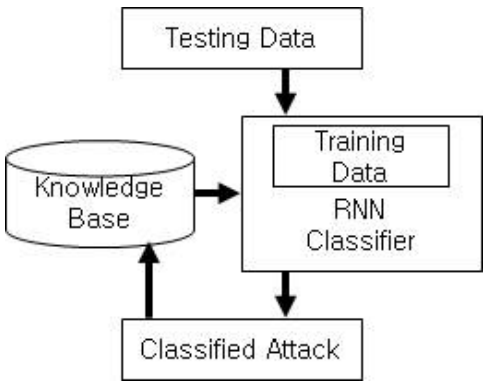
[Fig. 2] Membership function assignments for src_bytes

맴버십 함수는 매우 낮음, 낮음, 보통, 높음, 매우 높음의 다섯 단계로 구분하였다.

퍼지추론 시스템은 퍼지 로직을 사용하여 입력을 출력으로 변환하는 프로세스이고 집합 프로세서를 통해 맴버십 함수로 정의하였다. 계층적 분류자는 IF/ELSE IF.../ELSE를 사용하여 분류하였다.

4.2 RNN

"RNN을 이용한 공격 분류를 위한 지능형 침입탐지 시스템 모델"[2]은 지식 기반(Knowledge Base), 침입 탐지 신호 학습을 위한 RNN 기반 분류기, 침입 공격 탐지, IDS 데이터 집합(훈련 및 테스트)으로 구성되어 있다.



[Fig. 3] RNN Based IDS Model

RNN 기반 분류기는 해당 공격유형 기반으로 공격을 탐지하도록 훈련하는데 기여도 값이 모든 특징에 할당되어 있고 기여도 값이 누적 되면서 모든 공격에 정확한 예

측을 위해 임계값을 수정한다. RNN 분류기 메커니즘은 각 속성의 집합적 기여도 값을 기본으로 실행하고 '속성 선택' 측정값으로 공격을 탐지하고 규칙을 적용한다. 속성의 집합적 기여도가 임계치보다 높으면 공격으로 판단한다. 공격이 아닌 것은 지식 기반으로 식별할 수 있으며 공격 및 공격이 아닌 것은 지식 기반으로 업데이트 된다.

RNN 탐지 모델의 침입 탐지는 입력으로 KDD CUP 99 및 Knowledge Base, 출력은 침입으로 분류된 데이터 셋이다. 탐지의 순서는 1. 데이터를 읽고 2. Knowledge Base에서 지식을 추출한다. 3. 데이터 셋에서 분류를 위한 특징을 추출하고 4. 테스트 데이터 셋에 지식(RNN에서 훈련)을 적용한다. 5. 테스트 데이터를 읽고 6. 공격 또는 정상 데이터에 라벨을 수정한다. 7. 공격 패턴을 확인하기 위해 라벨 확인 8. 6 과 7에서 확인한 것은 Knowledge Base에 업데이트 한다. 9. 모든 훈련 데이터가 1-8단계를 수행하면 종료한다.

5. 침입탐지시스템 탐지 성능 비교

침입탐지 시스템의 성능을 평가하기 위해 ADR, FPR, Recall, Precision 등을 사용한다.

<Table 1> Confusion Matrix of Metrics calculations

	Classified as Normal	Classified as Attack
Normal	False Positive-FP	True Negative-TP
Attack	True Positive-TP	False Negative-FN

<Table 1>은 정상 및 공격 데이터를 정상 및 공격으로 분류하였을 경우의 분류 기준이다. 예를 들어 True Negative-TP는 정상 데이터를 공격데이터로 구분한 것이다.

ADR(Attack Detection Rate) : 공격 탐지율

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

FPR(False Positive Rate) : 정상 데이터 중 공격으로 잘 못 탐지한 비율

$$FPR = \frac{FP}{FP + TN} \times 100$$

Recall : 공격 데이터 중 공격으로 탐지한 비율

$$Recall = \frac{TP}{TP + FN} \times 100$$

Precision : 탐지한 데이터 중에서 정확하게 공격으로 탐지한 비율

$$\mathrm{Precision} = \frac{TP}{TP + FP} \times 100$$

5.1 퍼지

실험은 오픈 소프트웨어인 jFuzzyLogic을 사용하였고, 훈련데이터로 corrected.gz 사용하였고, kddcup.data 10 percent.gz으로 성능을 측정하였다.

<Table 2> Training results for corrected dataset

Layer	Attack type	Total records	Records detected correctly	Attack detection rate (%)
DoS	smurf	164,091	164,091	100.00
	neptune	58,001	57,402	98.97
	mailbomb	5,000	4,998	99.96
	back	1,098	1,079	98.27
	apache2	794	783	98.61
	teardrop	12	12	100.00
	Total	228,996	228,365	**99.72**
Probe	snmpgetattack	7,741	7,728	99.83
	guess_passwd	4,367	4,297	98.40
	Satan	1,633	1,620	99.20
	mscan	1,053	1,047	99.43
	saint	736	721	97.96
	portsweep	354	348	98.31
	ipsweep	306	301	98.37
	nmap	84	83	98.81
	Total	16,274	16,145	**99.21**
R2L	processtable	759	754	99.34
	pod	87	87	100.00
	snmpguess	2,406	2,404	99.92
	warezmaster	1,602	1,592	99.38
	Total	4,854	4,837	**99.38**

<Table 2>는 퍼지를 이용하여 Corrected.gz 데이터를 이용하여 훈련을 하였는데, 총38개의 공격 유형 중 18개만 제시하였다. 제시한 공격 유형에 대한 훈련 결과는 매우 좋은 것으로 나타났다.

<Table 3> Testing results for corrected 10% dataset

Layer	Attack type	Total records	Records detected correctly	Attack detection rate (%)
DoS	smurf	280,790	280,790	100.00
	neptune	107,201	106,019	98.90
	mailbomb	-	-	-
	back	2203	2151	97.64
	apache2	-	-	-
	teardrop	979	975	99.59
	Total	391,173	389,935	**99.68**
Probe	snmpgetattack	-	-	-
	guess_passwd	53	49	92.45
	satan	1589	1562	98.30
	mscan	-	-	-
	saint	-	-	-
	portsweep	1040	1021	98.17
	ipsweep	1247	1229	98.56
	nmap	231	226	97.84
	Total	4,160	4,087	**98.25**
R2L	processtable	-	-	-
	pod	264	264	100.00
	snmpguess	-	-	-
	warezmaster	20	20	100.00
	Total	284	284	**100.00**

<Table 3>은 훈련한 모델을 통해 10% 데이터 셋으로 테스트 한 결과 대체적으로 매우 우수한 결과가 나왔고, R2L공격 유형은 100% 탐지 결과가 나타났다.

mailbomb, apache2, snmpgetattack, mscan, saint, processtable, snmpguess의 공격은 10% 데이터 셋에는 존재하는 않는 공격유형이다.

다만, spy. warezclient의 공격은 10% dataset에 존재하지만 테스트 결과에는 제시되어 있지 않았다. 또한 공격 유형이 U2R인 공격 buffer_overflow, rootkit, loadmodule, perl은 탐지 결과가 제시되어 있지 않았다.

5.2 RNN

실험은 입력과 출력은 JAVA로 하고 데이터 마이닝 소프트웨어인 WEKA 툴을 사용하였다[8]. 훈련데이터로는 kddcup.data.gz를 사용하였고, kddccup.data 10 percent.gz으로 성능을 측정하였다.

<Table 4>는 퍼지 IDS와 RNN IDS의 탐지 결과 및 다른 IDS의 탐지 결과를 보여 주고 있다. RNN IDS는 C4.5, CRF와 비교하였을 경우 우수한 결과를 보이지만 퍼지 IDS와 비교하였을 경우 공격 유형 Probe, DoS는 다소 낮은 탐지율을 보이고 있다. 공격 유형 R2L은 퍼지가 매우 우수한 탐지 성능을 보이고 있었다. 다만 U2R의 공격 유형은 퍼지 IDS의 경우 제시되어 있지 않으므로 RNN IDS가 우수하다고 할 수 있다.

<Table 4> Performance Comparsion of Various Algorithms

Attacks	Probe	DoS	U2R	R2L
C4.5 (Decision Tree)	80.80	97.00	1.80	4.60
Conditional Random Field	98.60	97.40	86.30	29.60
RNN IDS	**96.66**	**97.40**	**86.50**	**29.73**
Fuzzy IDS	**98.25**	**99.65**	-	**100.00**

<Table 5> Compare Recall and Precision

Attack Type	Fuzzy IDS		RNN IDS	
	FPR	Recall	Recall	Precision
Probe	2.73	97.28	97.80	88.34
DoS	0.94	98.97	97.05	99.90
U2R	-	-	62.70	56.12
R2L	0.00	99.99	28.81	94.10

공격 데이터 중 공격으로 탐비한 비율인 Recall은 <Table 5>와 같다.

6. 결론

본 논문에서는 KDD CUP 99 데이터 셋으로 퍼지 및 RNN을 이용한 침입탐지 시스템을 비교하였다.

퍼지 IDS가 공격 유형 Probe, DoS, R2L에서 매우 우수한 탐지결과를 보이고 있고 공격 유형 U2R은 RNN IDS가 우수한 탐지를 보이고 있다.

KDD CUP 1999 데이터 셋을 이용하여 침입탐지에 관한 많은 연구가 이루어졌지만 kddcup.data.gz를 사용하여 훈련하고, kddccup.data 10 percent.gz를 이용한 성능 테스트와 더불어 corrected.gz를 사용하여 기존에 훈련하지 않은 새로운 공격 방법에 대한 탐지를 할 수 있는 연구가 많이 진행되어야 한다. 또한, 현재는 KDD CUP 1999 데이터 셋이 발표되었을 때보다 다양한 공격 기법이 존재하기 때문에 다양한 공격기법을 포함하는 데이터 셋이 필요하다. 그러므로 데이터 셋을 만드는 연구가 필요하다.

ACKNOWLEDGMENTS

This research was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government(MISP)(2016R1A4A1011761).

REFERENCES

[1] S. Ramakrishnan, S. Devaraju "Attack's Feature Selection-Based Network Intrusion Detection System Using Fuzzy Control Language" International Journal of Fuzzy Systems, 2016, 1-13.

[2] R. Bala Krishnan, N. R.Raajan "An Intellectual Intrusion Detection System Model for Attacks Classification using RNN" International Journal of Pharmacy & Technology, Vol. 8, No. 4, pp. 23157-23164

[3] KDD Cup 1999 Intrusion detection data: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[4] Chirag Modi, Dhiren Patel, Bhavesh Borissaniya, Hiren Patel, Avi Patel, Muttukrishnan Rajarajan, "A Survey of intrusion Detection techniques in Cloud", Journal of Network and Computer Application, Vol. 36, pp. 42-57, 2013.

[5] Saniee A. M., Mohamadi, H., Habibi, J.: Design and analysis of genetic fuzzy systems for intrusion detection in computer net- works. Expert Syst. Appl 38, 7067 - 7075 (2011)

[6] Wang, G., Hao, J., Ma, H., Huang, "A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering", Elsevier Expert Syst. Appl. Vol. 37, pp. 6225 - 6232, 2010.

[7]. Sheikhan, M., Jadidi, Z., Farrokhi, H., "A Intrusion detection using reduced-size RNN based on feature grouping", Neural Comput., Vol. 21, No. 6, pp. 1185 - 1190, 2010.

[8] Cingolani P.: jFuzzyLogic: open source fuzzy logic library and FCL language implementation (fcl code). http://jfuzzylogic.sour ceforge.net/html/exa-mple_fcl.html

[9] Gupta, K.K., Nath, B., Kotagiri, R., "Layered approach using conditional random fields for intrusion detection", IEEE Trans. Dependable Sec. Comput., No. 7, Vol. 1, pp. 35 - 49, 2010.

[10] Wei, N., Di, H., "A probability approach to anomaly detection with twin support vector machines", J. Shanghai Jiaotong Univ. (Sci.), Vol. 15, No. 4, pp. 385 - 391, 2010.

[11] Devaraju, S., Ramakrishnan, S., "Performance analysis of intrusion detection system using various neural network classifiers", IEEE Proc. Int. Conf. Recent Trends Info. Tech., No. 4, pp. 35 - 312, 2011.

[12] Anuar, N.B., Sallehudin, H., Gani, A., Zakari, O.," Identifying false alarm for network intrusion detection system using hybrid data mining and decision tree", Malays. J. Comput. Sci., Vol. 21, No. 2, pp. 101 - 115, 2008.

[13] Devaraju, S., Ramakrishnan, S., "Performance comparison for intrusion detection system using neural network with KDD dataset", ICTACT J. Soft Comput. Vol. 4, No. 3, pp. 743 - 752, 2014.

[14] Jiang, M., Gan, Z., Wang, C., Wang, Z., "Research of the intrusion detection model based on data mining", Elsevier Energy Proc Vol. 13, pp. 855 - 863, 2011.

[15] Tajbakhsh, A., Rahmati, M., Mirzaei, A., "Intrusion detection using fuzzy association rules", Elsevier Appl. Soft Comput. Vol. 9, pp. 462 - 469, 2009.

[16] Hyung-Jin Mun, Yooncheol Hwang, Ho-Yeob Kim, "Countermeasure for Prevention and Detection against Attacks to SMB Information System - A Survey," Journal of IT Convergence Society for SMB, Vol. 5, No. 2, pp. 1-6, 2015

[17] Miyea Shin, Sunghyuck Hong, "A Defending Method Against DDoS Attacks With Router Control," Journal of IT Convergence Society for SMB, Vol. 5, No. 1, pp. 21-26, 2015

[18] You-Dong Yun, "Development of Smart Senior Classification Model based on Activity Profile Using Machine Learning Method", Journal of the Korea Convergence Society, Vol. 8. No. 1, pp. 25-34, 2017.

[19] Myung-Seong Yim, “Development of Measures of Information Security Policy Effectiveness To Maximize the Convergence Security”, Journal of the Korea Convergence Society, Vol. 5, No. 4, pp. 27-32, 2014.

양 은 목(Yang, Eun Mok)

・2000년 2월 : 한밭대학교 전자계산학과(학사)
・2002년 2월 : 공주대학교 전자계산학과(석사)
・2016년 8월 : 공주대학교 수학과(박사)
・관심분야 : 정보보안, 통계, 빅데이터, 등
・E-Mail : emyang@kongju.ac.kr

이 학 재(Lee, Hak Jae)

・1987년 2월 : 호남대 영어영문학과 졸업(문학사)
・2014년 8월 : 전남대학교 대학원 전자공학과 졸업(공학석사)
・2015년 3월 ~ 현재 : 전남대학교 전자컴퓨터공학과 박사과정 재학 중
・관심분야 : RF Circuit(RFIC), 근거리무선통신, 임베이드 시스템
・E-Mail : hjlee5120@hamail.net

서 창 호(Seo, Chang Ho)

・1990년 2월 : 고려대학교 수학과(학사)
・1992년 2월 : 고려대학교 수학과(석사)
・1996년 8월 : 고려대학교 수학과(박사)
・1996년 8월 ~ 2000년 2월 : 한국전자통신연구원 선임연구원, 팀장
・2000년 3월 ~ 현재 : 공주대학교 응용수학과(정보보호전공), 융합과학과 교수
・관심분야 : 암호알고리즘, PKI, 무선 인터넷 보안 등
・E-Mail : chseo@kongju.ac.kr