Regular paper | Journal of the KIECS. pp. 249-256, vol. 19, no. 1, Feb. 29. 2024, t. 123, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2024.19.1.249

특징학습과 계층분류를 이용한 침입탐지 방법 연구

이한성* · 정윤희** · 정세훈***

Intrusion Detection Approach using Feature Learning and Hierarchical Classification

Han-Sung Lee* · Yun-Hee Jeong** · Se-Hoon Jung***

요 약

기계학습 기반의 침입탐지 방법론들은 분류하고자 하는 각 클래스에 대해 균등한 많은 학습 데이터가 필요하며, 탐지 또는 분류하려는 공격유형의 추가 시 시스템을 모두 재학습해야 하는 문제점을 가지고 있다. 본 논문에서는 특징학습과 계층분류 방법을 이용하여, 비교적 적은 학습 데이터를 이용한 분류 문제 및 데이터 불균형 문제를 해결하고, 새로운 공격유형의 추가가 쉬운 침입탐지 방법론을 제안하고자 한다. 제안된 시스템은 KDD 침입탐지 데이터를 이용한 실험으로 가능성을 검증하였다.

ABSTRACT

Machine learning-based intrusion detection methodologies require a large amount of uniform learning data for each class to be classified, and have the problem of having to retrain the entire system when adding an attack type to be detected or classified. In this paper, we use feature learning and hierarchical classification methods to solve classification problems and data imbalance problems using relatively little training data, and propose an intrusion detection methodology that makes it easy to add new attack types. The feasibility of the proposed system was verified through experiments using KDD IDS data..

키워드

Cyber Security, Intrusion Detection, Feature Learning, Hierarchical Classification
사이버 보안, 침입 탐지, 특징 학습, 계층적 분류

Ⅰ. 서 론

최근 사이버 공간상에서 목표 시스템에 피해를 주거나 목표 시스템이 가지고 있는 중요 자산정보를 탈취하기 위한 사이버 공격이 급속도로 증가하고 있으며, 그 피해도 커지고 있다. 사이버 공격은 시스템 내 단말의 취약성(Vulnerability)을 이용하여 이루어지며, 중요한 자산을 가지고 있는 목표 장비가 일차적으로 보호되고 있다고 하더라도 조직 내부의 취약한 장비를 통해 목표 시스템에 접근할 수 있다면 해당 시스템을 보호할 수 없다는 문제점을 가지고 있다[1-4].

앞서 설명한 문제를 해결하기 위하여 다양한 네트워크 침입탐지 방법론들이 제안되었다. 초기 침입탐지 모델은 규칙 기반 방법을 사용하여 오용탐지(Misuse

* 안동대학교 창의융합학부(mohan@anu.ac.kr)
** 안동대학교 멀티미디어공학과(tkmsze@gmail.com)
*** 교신저자 : 순천대학교 컴퓨터공학과
· 접 수 일 : 2023. 12. 05
· 수정완료일 : 2024. 01. 08
· 게재확정일 : 2024. 02. 17
· Received : Dec. 05, 2023, Revised : Jan. 08, 2024, Accepted : Feb. 17, 2024
· Corresponding Author : Se-Hoon Jung
Dept. Computer Engineering, Sunchon University,
Email : shjung@scnu.ac.kr

Detection) 및 이상 행위 탐지(Anomaly Detection)를 수행하였다. 그러나 규칙 기반 방법론들은 기존에 발견하지 못한 새로운 공격유형 및 기존 공격 방법의 변이에 대한 탐지가 불가능하다는 문제점을 가지고 있다. 규칙 기반 방법론의 한계를 극복하기 위하여 기계학습, 소프트 컴퓨팅(Soft Computing), 데이터마이닝을 기반으로 한 많은 침입탐지 방법론들이 제안되었으나[5-10], 기계학습을 이용한 네트워크 침입탐지 방법론들은 네트워크 데이터와 기계학습 방법론이 가지고 있는 구조적 문제점에 직면해 있다[11-12]. 첫 번째로 학습 데이터가 불균형(Data Imbalance)하거나 학습 데이터가 적은 경우는 학습이 어렵다는 문제점을 가지고 있다. 두 번째로 새롭게 추가되는 클래스를 학습하기 위하여 기존의 모델을 새롭게 재학습해야 하는 문제점을 가지고 있다.

본 논문에서는 특징학습(Feature learning) 기술과 계층분류 기반 침입탐지 방법론을 제안한다. 제안하는 방법은 우선 정상 데이터와 상위 공격유형인 DoS(: Denial of Service), R2L(: Root to Local attacks), L2R(: User to Root attack), 조사(Probe) 공격을 분류한다. 다음 단계로 각 공격유형 별 세부 공격유형을 분류하는 계층적 구조를 갖는다. 클래스별 불균형한 적은 데이터를 이용하여 분류 모델을 구성하고, 세부 분류를 수행하기 위하여 kNN(k Nearest Neighborhood) 알고리즘을 기본 분류기로 활용하였으며, kNN[13-14] 알고리즘의 상대적 낮은 분류 성능을 극복하기 위하여 특징학습을 적용하였다. 제안하는 방법은 새로운 공격유형이 발견되더라도 쉽게 시스템에 반영할 수 있는 구조로 되어 있다.

본 연구에서는 KDD 침입탐지 데이터를 이용하여 제안된 알고리즘의 검증을 진행하였다. 실험 결과 본 연구에서 제안하는 방법이 적은 학습 데이터로도 침입탐지를 수행할 수 있으며, 새로운 공격이 유형이 발견되어 매우 적은 데이터를 확보하여도 시스템을 구축할 수 있음을 보였다.

II. 특징학습을 이용한 계층분류 기반 침입탐지

2.1 전체 구조

사이버 공격 데이터는 네트워크의 특성상 데이터의 인스턴스가 많은 공격유형과 데이터 인스턴스가 많지 않은 공격유형으로 나눌 수 있다. 예를 들어 DoS 공격의 경우는 매우 많은 데이터 인스턴스를 발생하지만 R2L 또는 L2R 공격의 경우는 매우 적은 데이터 인스턴스를 발생시킨다. 따라서 클래스별로 학습 데이터가 불균일한 학습 데이터 불균형 문제를 내포하고 있으며, 학습 데이터가 적은 경우는 학습이 어렵다. 또한, 정보통신 기술 및 인공지능 기술의 발전으로 인하여 기존에 알려지지 않은 새로운 공격유형과 지능화된 공격 방법이 빠른 속도로 새롭게 등장하고 있다. 따라서, 새로 발견된 적은 수의 공격 데이터를 시스템에 빠르게 추가하여야 한다.

위에서 언급한 침입탐지 문제를 해결하기 위하여 본 논문에서는 kNN 알고리즘을 기본 분류 알고리즘으로 적용하였으며, 분류 성능을 높이기 위하여 심층신경망(Deep Neural Network)을 이용하여 특징학습을 수행한다. 아래 그림 1.은 제안하는 침입탐지 접근 방법의 전체 구조도이다.

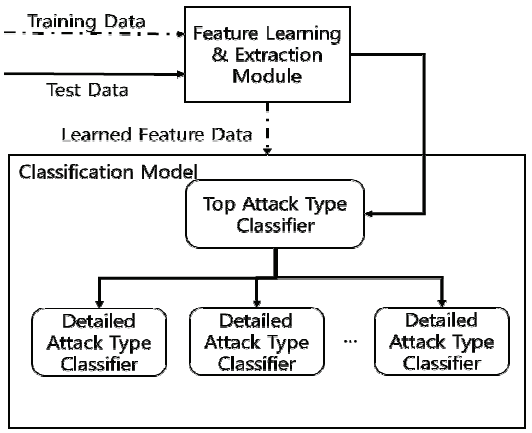

그림 1. 제안하는 방법 전체 구조도
Fig. 1 Overall architecture of the proposed approach

첫 번째 단계로, 심층신경망을 이용하여 특징학습 및 특징 추출을 수행하고 분류기를 구성한다. 학습 데이터를 이용하여 상위 공격유형인 DoS, R2L, L2R, 조사 공격을 분류하도록 심층신경망을 학습한다. 학습이 완료되면 학습 데이터를 심층신경망에 입력하여 마지막 은닉층의 출력을 특징으로 추출한다. 추출된 특징을 이용하여 앞서 설명한 상위 공격유형을 분류

할 수 있는 상위 공격 분류기를 구축한다. 각 공격 별 세부 클래스를 기준으로 DoS 공격의 세부 공격유형 분류를 위한 세부 분류기를 포함하여, R2L, L2R 및 조사 공격을 위한 세부 분류기를 구축한다. 다음 단계로, 실제 분류를 위한 테스트 데이터를 심층신경망에 입력하여 특징을 추출한다. 추출된 특징을 상위 공격 분류기로 분류하고, 분류된 상위 공격에 해당하는 세부 분류기를 통하여 구체적인 공격유형을 분류한다.

2.2 특징학습 및 특징 추출

앞에서 설명한 바와 같이 특징학습 및 특징 추출을 위하여 심층신경망을 이용한다. 본 논문에서는 입력 데이터의 차원은 41차원이며, 512개의 뉴런을 갖는 은닉층1, 512개의 뉴런을 갖는 은닉층2, 1024개의 뉴런을 갖는 은닉층3, 1024개의 뉴런을 갖는 은닉층4와 5개의 클래스를 분류하는 출력층으로 구성된다. 은닉층에서는 활성화 함수로 ReLU 함수를 사용하였으며, 출력층은 softmax 함수를 사용하였다. 아래 그림 2.는 특징학습 및 특징 추출을 위한 심층신경망이다.

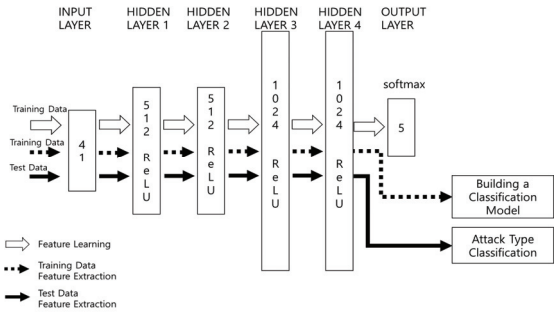

그림 2. 특징학습 및 특징 추출 모델
Fig. 2 Feature learning and feature extraction model

특징학습 단계에서는 심층신경망을 학습 데이터를 사용하여 5개의 상위 공격유형을 분류하도록 학습한다. 본 연구에서는 최적화 방법으로 Aadm을 사용하였으며, Loss 함수로는 Sparse Categorical Cross Entropy를 사용하였다. 특징학습이 완료되면 학습 데이터를 입력으로 은닉층4의 출력을 저장하여 특징을 추출한다. 추출된 특징을 이용하여 상위 공격 분류기 및 각 공격유형 별 세부 분류기들을 생성한다. 공격 탐지 및 분류 단계에서는 실제 분류를 수행할 공격 데이터(테스트 데이터)를 입력으로 특징을 추출한다. 추출된 특징을 분류기에 입력하여 공격 탐지 및 세부 유형 분류를 수행한다.

2.3 kNN을 이용한 계층적 분류 모델

kNN 알고리즘은 게으른 학습자 (Lazy Learner)로 별도의 학습 과정이 없으며, 적은 데이터 및 불균형 데이터를 이용하여 학습 데이터를 구성하더라도 분류기를 만들고 수행할 수 있다는 장점이 있다. 또한, 기존의 분류기에 새로운 클래스를 추가할 때 단순히 학습 데이터에 새로운 클래스에 해당하는 데이터와 라벨을 추가함으로써, 별도의 학습 과정 없이 분류기를 사용할 수 있다. kNN 알고리즘은 많은 장점에도 불구하고 다른 기계학습과 비교하여 상대적으로 낮은 성능을 보이고 있지만, 특징학습 및 특징 추출을 도입하여 어느 정도 문제를 해결할 수 있다.

제로데이 공격을 포함하는 새로운 공격유형이 보고되면 다음의 절차에 따라 침입탐지 상위 공격 분류기와 세부 분류기를 재구성한다. 첫째, 만약 보고된 공격유형이 기존의 상위 공격유형의 범주에 속하면 발견된 공격 데이터를 특징 추출 모듈에 입력하여 특징을 추출한다. 추출된 특징을 해당 상위 공격유형에 해당하는 세부 분류기의 학습 데이터에 추가하여 세부 분류기를 재구성한다. 둘째, 만약 보고된 공격유형이 기존의 상위 공격유형의 범주에 속하지 않는 새로운 상위 공격유형이라면 발견된 공격 데이터를 특징 추출 모듈에 입력하여 특징을 추출하고 상위 공격 분류기의 학습 데이터에 추가하여 상위 공격 분류기를 재구성한다. 재구성된 상위 공격 분류기의 서비스를 지속하는 동시에 특징학습 및 특징 추출 모듈을 재학습한다. 특징학습 및 특징 추출 모듈이 학습되는 동안에도 침입탐지 및 공격 데이터 분류 서비스를 지속해서 제공할 수 있으며 특징학습 및 특징 추출 모듈의 학습이 완료되면 시스템을 재구성하여 성능의 저하를 막을 수 있다.

본 연구에서 kNN 알고리즘을 기본 분류 알고리즘으로 활용함으로써, 제안하는 침입탐지 방법론은 다음과 같은 특징을 갖는다. 첫째, 침입탐지 시스템 구축 초기 단계에서 겪게 되는 학습 데이터 부족 및 불균형 문제를 해결할 수 있다. 둘째, 지속해서 증가하는 새로운 공격유형들을 시스템에 쉽게 추가하여 침입탐지 시스템의 성능을 안정적으로 유지할 수 있다.

III. 실험 결과 및 분석

3.1 데이터 및 실험 설계

본 연구에서는 KDD 침입탐지 데이터[11, 15-16]를 이용하여 실험을 수행하였다. KDD 침입탐지 데이터는 DARPA Intrusion Detection Evaluation Program에 의해 표준 데이터 집합을 얻기 위하여 미국 군사 네트워크상에서 시뮬레이션을 통하여 만들어졌다. 총 속성은 42차원으로 구성되어 있으며, 9개의 기호형 속성과 32개의 숫자형 속성, 그리고 공격 라벨로 구성된다. 데이터는 크게 전체 데이터, 전체 데이터의 10% 샘플링된 데이터, 테스트를 위해 정확하게 라벨링 된 데이터로 구성되어 있다. KDD 데이터는 크게 4개의 공격유형인 DoS, R2L, L2R, 조사 공격으로 구성되어 있다. 각 공격 유형별 데이터 인스턴스 개수가 매우 불균형을 이루고 있으며, 특정 공격(R2L 및 L2R)의 경우 공격 데이터 자체도 데이터가 적지만 세부 공격 유형별로 매우 적은 데이터로 구성되어 있다. 따라서, 본 연구에서 제안하는 방법론을 검증하기 위하여 KDD 데이터를 사용하였다. 특징학습 및 계층분류기를 구축하기 위하여 KDD 데이터 중 정확하게 레이블링 된 10% 훈련 데이터셋을 사용하였으며, 테스트를 위하여 정확하게 레이블링 된 테스트 데이터셋의 일부를 사용하였다. 학습 데이터와 테스트 데이터 모두 U2R 공격 데이터, R2L 공격 데이터, 조사 공격 데이터로 구성되어 있다. 반면, 상대적으로 데이터양이 많은 정상 데이터 일부를 랜덤 선택하였으며, DoS 공격 데이터는 세부 공격 별 데이터 일부를 랜덤으로 선택하였다.

3.2 상위 공격유형 분류 결과

아래의 표 1은 kNN 알고리즘, 2.2절에서 설명한 심층신경망, 그리고 본 논문에서 제안하는 방법론을 이용한 상위 공격유형 분류 결과이다. 실험 결과를 분석하여 보면, kNN 알고리즘은 상대적으로 적은 데이터를 포함하고 있는 U2R 공격 분류에서 심층신경망과 비교하여 좋은 성능을 보였다. 반면 다른 공격유형의 분류에서는 심층신경망 및 제안하는 방법에 비해 낮은 성능을 보였다. 심층신경망의 경우는 kNN 알고리즘과 비교하여 전체적으로 좋은 성능을 보였지만, 데이터 개수가 적은 U2R 공격과 R2L 공격에서는 낮은 성능을 보였다. 제안하는 방법론은 kNN 알고리즘 및 심층신경망과 비교하여 전반적으로 우수한 성능을 보이고 있음을 확인할 수 있다. 본 논문에서 제안하는 방법은 kNN의 적은 데이터 및 불균형 데이터를 처리할 수 있는 능력에 특징학습을 통한 분류 성능을 높인 알고리즘으로, 침입탐지 분야뿐만 아니라 적은 데이터와 데이터 불균형 특성이 있는 불량품 탐지를 위한 비전 검사 분야 등 다양한 분야에 적용 가능할 것으로 판단된다.

표 1. 상위 공격유형 분류 결과
Table 1. Top attack type classification results

Attack Type	kNN	Deep Learning	Proposed Approach
Normal Data	98.9	98.9	98.9
DoS Attack	95.8	99.4	99.6
U2R Attack	45.0	40.0	47.5
R2L Attack	19.2	20.2	25.8
Probe Attack	84.3	87.8	84.3
Total	72.9	74.6	75.9

표 2에 GAN을 이용한 데이터 증강을 통한 분류 성능 개선[11] 방법, 침입탐지를 위하여 개발된 PLS SVM[15] 및 랜덤 포레스트(Random Forest)를 이용한 방법[16] 등 문헌조사를 통한 다른 방법론들과의 연구 결과 비교를 제시하였다.

표 2. 문헌의 다른 연구 결과와의 비교
Table 2. Comparison with other published methods

Attack Type	GAN [11]	PLSSVM [15]	RF [16]	Proposed Approach
Normal Data	82.8	95.6	91.0	98.9
DoS Attack	99.4	78.7	98.9	99.6
U2R Attack	N/A	30.7	100	47.5
R2L Attack	83.7	84.8	66.6	25.8
Probe Attack	99.3	86.4	55.1	84.3
Total	N/A	N/A	N/A	75.9

각 연구의 해결하고자 하는 문제 정의, 실험 방법 및 데이터의 차이가 존재하여 직접적인 성능 평가는 어렵지만 다른 방법론과의 장단점 비교 및 제안하는 방법론의 특성을 파악하는 데 사용될 수 있을 것으로 판단된다. 문헌의 다른 연구 결과와 제안된 방법을 비교하면 제안된 방법이 정상 데이터 및 DoS 공격 분류에서는 우수한 성능을 보이지만 R2L 공격 분류에서는 낮은 성능을 보였다.

3.3 침입탐지 세부 분류 성능

제안하는 방법론의 공격 유형별 세부 분류 능력을 확인하기 위하여 각 공격 유형별로 데이터를 나누고 세부 유형으로 분류기를 구성하였다. 심층신경망의 경우는 세부 유형에 대해 학습이 이루어지지 않았으며, 문헌상의 다른 연구 결과도 대부분 상위 공격유형 분류에 집중된다. 심층신경망의 세부 분류 능력 비교가 어려워 단순 kNN 알고리즘과 제안된 방법 두 가지의 분류 성능을 제시한다.

표 3은 DoS 공격의 세부 공격유형 6가지를 분류한 결과이다. DoS 공격의 세부 공격유형 분류에서는 단순 kNN 알고리즘과 제안하는 방법이 거의 비슷한 성능을 보인다.

표 3. DoS 공격 세부 공격유형 분류 결과
Table 3. Detailed attack type classification results of DoS attacks

Attack Type	Simple kNN	Proposed Approach
Back Attack	100	100
Land Attack	100	100
Neptuen Attack	100	99.8
Pod Attack	100	100
Smurf Attack	100	100
Teardrop Attack	92.3	92.3
Total	99.9	99.9

표 4는 U2R 공격의 세부 공격유형 4가지를 분류한 결과이다. U2R 공격은 세부 공격 유형별 데이터가 가장 적은 공격유형이다. U2R 공격의 세부 공격유형 분류에서는 제안하는 방법론이 우수한 성능을 보인다. Load Module 공격의 경우 두 가지 방법론 모두 분류에 실패하였다. 해당 공격의 경우 데이터 개수가 2개이며 두 방법 모두 분류에 실패하였다. 제안된 방법은 특히, Buffer Overflow 공격과 Rootkit 공격 분류에서 더 우수한 성능을 보였다.

표 4. U2R 공격 세부 공격유형 분류 결과
Table 4. Detailed attack type classification results of U2R attacks

Attack Type	Simple kNN	Proposed Approach
Buffer Overflow Attack	31.8	77.2
Load Module Attack	0	0
Perl Attack	50.0	50.0
Rootkit Attack	64.3	78.6
Total	42.5	72.5

표 5는 R2L 공격의 세부 공격유형 6가지를 분류한 결과이다. R2L 공격의 세부 공격유형 분류에서도 제안하는 방법론이 우수한 성능을 보인다. Ftp Write 공격과 Imap 공격의 경우 두 가지 방법론 모두 분류에 실패하였다. 두 공격은 각각 데이터 개수가 3개, 1개이다. 제안된 방법은 Guess Password 공격과 Warezmaster 공격 분류에서 더 우수한 성능을 보였으나, Multihop 공격 분류에서는 단순 kNN이 우수한 성능을 보였다.

표 5. R2L 공격 세부 공격유형 분류 결과
Table 5. Detailed attack type classification results of R2L attacks

Attack Type	Simple kNN	Proposed Approach
Ftp Write Attack	0	0
Guess Password Attack	0.6	14.7
Imap Attack	0	0
Multihop Attack	22.2	16.6
Phf Attack	50.0	50.0
Warezmaster Attack	54.2	94.8
Total	15.08	36.1

표 6은 조사 공격의 세부 공격유형 4가지를 분류한 결과이다. 조사 공격의 세부 공격유형 분류에서는 제안하는 방법이 전반적으로 우수한 성능을 보인다.

표 6. 조사 공격 세부 공격유형 분류 결과
Table 6. Detailed attack type classification results of Probe attacks

Attack Type	Simple kNN	Proposed Approach
Ip sweep Attack	98.0	99.0
Nmap Attack	100	100
Port sweep Attack	94.9	97.4
Satan Attack	99.8	99.5
Total	98.8	99.1

실험 결과를 분석하여 보면, 본 논문에서 제안하는 특징학습과 계층적 분류 방법은 다른 기계학습 알고리즘 및 심층신경망으로는 분류하기 어려운 침입탐지 상위 공격의 세부 공격유형을 분류할 가능성을 보여주고 있다. 극히 적은 데이터를 포함하는 세부 공격유형의 경우 제안하는 방법으로도 분류하기 어렵다는 점을 발견하였지만, 특징학습 방법의 개선으로 어느 정도 극복할 수 있을 것으로 기대한다.

Ⅳ. 결론 및 향후 개선 방향

본 논문에서는 네트워크 공격 데이터의 특성으로 인한 기존 기계학습 기반의 침입탐지 방법론의 한계를 극복하기 위한 특징학습과 계층분류 모델 기반 침입탐지 모델을 제안하였다. 제안하는 침입탐지 방법론은 침입탐지 시스템 구축 초기 단계에서 겪게 되는 학습 데이터 부족 및 불균형 문제를 해결할 수 있으며, 지속해서 증가하는 새로운 공격유형들을 시스템에 쉽게 추가하여 침입탐지 시스템의 성능을 안정적으로 유지할 수 있다. 향후 개선 방향으로는 조금 더 분류 성능을 높일 수 있는 특징학습 기술에 관한 추가적인 연구와 적은 데이터와 데이터 불균형 문제를 내포하고 있는 비전 검사를 이용한 불량품 탐지 분야로의 적용 연구를 진행할 계획이다.

감사의 글

이 논문은 2021학년도 안동대학교 학술연구조성비에 의하여 연구되었음

References

[1] M. Macas, C. Wu, and W. Fuertes, “A survey on deep learning for cybersecurity: Progress, challenges, and opportunities,” *Computer Networks*, vol. 212, 2022, pp. 1-33.

[2] Y. Chun, “Hacking Detection Mechanism of Cyber Attacks Modeling,” *J. of the Korea Institute of Electronic Communication Sciences,* vol. 8, no. 9, 2013, pp. 1313-1318.

[3] M. Ahsan, K. E. Nygard, R. Gomes, M. M. Chowdhury, N. Rifat, and J. F. Connolly, “Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning－A Review,” *J. of Cybersecurity and Privacy*, vol. 2, no. 3, 2022, pp. 527-555.

[4] H. Liu and B. Lang, “Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey,” *Applied Sciences*, vol. 9, no. 20, 2019, pp. 1-28.

[5] P. Toupas, D. Chamou, K. M. Giannoutakis, A. Drosou, and D. Tzovaras, “An Intrusion Detection System for Multi-Class Classification based on Deep Neural Networks,” In *Proc. International Conf. on Machine Learning and Applications*, Boca Raton, FL, USA, Dec. 2019.

[6] Y. Lee, “A Design and Analysis of Multiple Intrusion Detection Model,” *J. of the Korea Institute of Electronic Communication Sciences,* vol. 11, no. 6, 2016, pp. 619-626.

[7] Y. Zeng, H. Gu, W. Wei, and Y. Guo, “Deep－Full－Range : A Deep Learning Based Network Encrypted Traffic Classification and Intrusion Detection Framework,” *IEEE Access*, vol. 7, 2019, pp. 45182-45190.

[8] N. N. Tran, R. Sarker, and J. Hu, “An Approach for Host-Based Intrusion Detection System Design Using Convolutional Neural Network,” In *Proc. of the Int. Conf. Mobile Networks and Management*, Chiba, Japan, Sept. 2017, pp. 116-126.

[9] A. Tuor, S. Kaplan, B. Hutchinson, N. Nichols,

and S. Robinson, “Deep learning for unsupervised insider threat detection in structured cybersecurity data streams,” In *Proc. Works. AAAI Conf. AI*, San Francisco, USA, Feb. 2017.

[10] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, “Deep Learning Approach for Intelligent Intrusion Detection System,” *IEEE Access*, vol. 7, 2019, pp. 41525-41550.

[11] H. Zhang, X. Yu, P. Ren, C. Luo, and G. Min, “Deep Adversarial Learning in Intrusion Detection: A Data Augmentation Enhanced Framework,” *ArXiv, abs/1901.07949,* vol. 3, 2019.

[12] J. Song, X. Wang, M. He, and L. Jin, “CSK-CNN: Network Intrusion Detection Model Based on Two-Layer Convolution Neural Network for Handling Imbalanced Dataset,” *Information*, vol. 14, no. 2, 2023, p. 1-17.

[13] J. Kwon and S. Cho, “Performance Analysis of Fingerprinting Method for LTE Positioning according to W-KNN Correlation Techniques in Urban Area,” *J. of the Korea Institute of Electronic Communication Sciences,* vol. 16, no. 6, 2021, pp. 1059-1068.

[14] K. Kim, J Kang, S. Han and J Park, “Development of Machine Learning-based Flood Depth and Location Prediction Model,” *J. of the Korea Institute of Electronic Communication Sciences,* vol. 18, no. 1, 2023, pp. 91-98.

[15] F. Amiri, M. M. R. Yousefi, C. Lucas, A. Shakery, and N. Yazdani, “Mutual information-based feature selection for intrusion detection systems,” *J. Network and Computer Applications*, vol. 34, no. 4, 2011, pp. 1184-1199.

[16] M. A. M. Hasan, M. Nasser, B. Pal, and S. Ahmad, “Support vector machine and random forest modeling for intrusion detection system (IDS),” *J. Intelligent Learning Systems and Applications*, vol. 6, no. 1, 2014, pp. 45-52.

저자 소개

이한성(Han-Sung Lee)

1996년 고려대 전산학과 (이학사)
2002년 고려대 전산학과 (이학석사)
2008년 고려대 전산학과 (이학박사)
2021년 ~ 현재 안동대학교 창의융합학부 조교수

※ 관심 분야 : 사이버 보안, 침입탐지, 멀티미디어 마이닝, 기계학습 및 딥러닝

정윤희(Yun-Hee Jeong)

2020년 ~ 현재 안동대학교 멀티미디어공학과 재학

※ 관심 분야 : 사이버 보안, 침입탐지, 빅데이터 분석, 기계학습 및 딥러닝

정세훈(Se-Hoon Jung)

2010년 순천대 멀티미디어공학과 (공학사)
2012년 순천대 멀티미디어공학과 (공학석사)
2017년 순천대 멀티미디어공학과 (공학박사)
2018년 8월 ~ 2020년 2월 영산대학교 빅데이터융합전공 조교수
2020년 3월 ~ 2022년 8월 안동대학교 창의융합학부 조교수
2022년 9월 ~ 현재 순천대학교 컴퓨터공학과 조교수

※ 관심 분야 : 사이버 보안, 강화학습, 데이터 마이닝, 딥러닝, 빅데이터 분석 및 예측