J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

이상 탐지 분석에서 알려지지 않는 공격을 식별하기 위한 이산 웨이블릿 변환 적용 연구☆

Application of Discrete Wavelet Transforms to Identify Unknown Attacks in Anomaly Detection Analysis

김 동 욱[1] 신 건 윤[1] 윤 지 영[3] 김 상 수[2] 한 명 묵[3*]
Dong-Wook Kim Gun-Yoon Shin Ji-Young Yun Sang-Soo Kim Myung-Mook Han

요 약

사이버 보안의 침입탐지 시스템에서 알려지지 않는 공격을 식별하기 위한 많은 연구가 이루어지고 있지만, 그 중에서도 이상치를 기반으로 하는 연구가 주목받고 있다. 이에 따라 우리는 알려지지 않는 공격에 대한 범주를 정의하여 이상치를 식별한다. 알려지지 않는 공격은 2가지 범주로 조사하였는데, 첫째는 변종 공격을 생성하는 사항이 있고, 두 번째는 새로운 유형으로 분류하는 연구로 나누었다. 우리는 변종 공격을 생성하는 연구 범주에서 변종과 같이 유사 데이터를 식별할 수 있는 이상치 연구를 수행하였다. 침입탐지 시스템에서 이상치를 식별하는 큰 문제는 정상행동과 공격행동이 같은 공간을 공유하는 것이다. 이를 위해 우리는 이산 웨이블릿 변환으로 정상과 공격에 대해 명확한 유형으로 나눌 수 있는 기법을 적용하고 이상치를 탐지하였다. 결과로 우리는 이산 웨이블릿 변환으로 재구성된 데이터에서 One-Class SVM을 통한 이상치를 식별 할 수 있음을 확인하였다.

☞ 주제어 : 알려지지 않는 공격, 이산 웨이블릿 변환, 이상 탐지, One-Class SVM

ABSTRACT

Although many studies have been conducted to identify unknown attacks in cyber security intrusion detection systems, studies based on outliers are attracting attention. Accordingly, we identify outliers by defining categories for unknown attacks. The unknown attacks were investigated in two categories: first, there are factors that generate variant attacks, and second, studies that classify them into new types. We have conducted outlier studies that can identify similar data, such as variants, in the category of studies that generate variant attacks. The big problem of identifying anomalies in the intrusion detection system is that normal and aggressive behavior share the same space. For this, we applied a technique that can be divided into clear types for normal and attack by discrete wavelet transformation and detected anomalies. As a result, we confirmed that the outliers can be identified through One-Class SVM in the data reconstructed by discrete wavelet transform.

☞ keyword : Unknown Attack, discrete wavelet transform, Anomaly Detection, One-Class SVM

1. 서 론

오늘날 정보기술은 현대 사회구조에 중요한 역할을 하고 있다. 스마트 시티, 스마트 그리드, 가상 발전소 또는 지능형 교통 시스템과 같은 첨단 인프라 개념을 위한 핵심 기술로서 사물 인터넷(IoT)의 채택이 진행됨에 따라 인터넷에 연결된 호스트 수는 기하급수적으로 증가할 것으로 예상된다.

사이버 공간에서의 사이버 보안은 광범위한 상호연결 네트워크 속에서 많은 위협요소에 노출되어 있다. 위협요소에 대응하기 위해 전 세계의 많은 보안 회사들은 네트워크 침입 공격과 악성 프로그램 감염으로부터 컴퓨터 장치, 네트워크 및 소프트웨어 응용 프로그램을 보호하기 위한 새로운 기술 설계에 주력하고 있다. 이 같은 사이버 보안 시스템은 네트워크 보안 시스템과 호스트 보안 시스템으로 구성된다. 이들 각각은 최소한 방화벽, 바이러스 백신 소프트웨어 및 침입 탐지 시스템(Intrusion Detection Systems, IDS)을 갖추고 있다.

1 Department of Computer Engineering, Gachon University, Sungnam-si, 13120, Korea
2 Agency for Defense Development Songpa P.O Box 132, Seoul, 05661 Korea
3 Department of Software, Gachon University, Sungnam-si, 13120, Korea
* Corresponding author (mmhan@gachon.ac.kr)
[Received 26 February 2021, Reviewed 17 March 2013, Accepted 29 March 2021]
☆ 이 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2018R1D1A1B07050864).
☆ 이 논문은 국방과학연구소 지원을 받아 수행된 연구임 (UD200020ED)

침입탐지 시스템의 목표는 서로 다른 종류의 악의적인 네트워크 트래픽과 컴퓨터 사용을 식별하는 것으로, 컴퓨터 시스템의 가용성, 무결성 또는 기밀성을 훼손하는 행위에 보호를 달성하는 것이다[1]. 이러한 사이버보안 배경 속에서 침입탐지 시스템을 통한 방어는 주요 사이버 침해사고에 대해 많은 분석정보를 제공받을 수 있다. 데이터 개체는 침입탐지 시스템에서 가장 기본적인 요소로, 공격 행동과 관련된 특징을 가지고 있다. 특징 유형과 특징 추출 방법은 데이터 요소마다 다르기 때문에 적절한 분석을 위한 기계 학습 모델도 달라진다. 최초의 기계학습 알고리즘을 이용한 네트워크 침입 감지는 Lee와 Stoflo[2]을 통해 프레임워크가 발간되었다. 이후 발전을 통해 IDS의 데이터 요소는 공격의 패턴으로 정의되는 특성에 따라 오용 검출(Misuse Detection)과 이상 검출(Anomaly Detection)로 나눌 수 있다[3]. 오용 검출은 패턴이나 승인되지 않는 의심스러운 행동을 기초로 학습하여 탐지가 이루어지고, 이상 탐지는 정상과 비정상 사이의 명확한 경계를 결정하는데 의존하여, 정상 동장의 프로필이 비정상 동작과의 크게 다를 경우로 분류한다. 단 정상 프로필은 매우 명확하게 기준 집합을 만족하는 것이 중요하다. 이처럼 침입탐지 시스템에서는 다양한 행위를 효과적으로 분류하기 위해 기계학습을 적용하기 있지만, 공격자의 악성 행위도 지속적으로 복잡해지고 있다.

기계학습을 이용한 사이버 보안은 알려진 공격과 알려지지 않는 공격의 유형으로 나뉠 수 있는데, 학습 데이터를 기반으로 수행하는 기계학습 모델은 알려지지 않는 공격에 대해서 취약하다. 하지만 이상탐지(Anomaly Detection) 영역에서는 알려지지 않는 공격을 탐지하기 위한 방법으로 정상 동작의 기준에 만족하지 않는 사항을 처리하는 것으로 가능하다. 그러나 이 방법에서도 한계점은 존재한다. 정상 프로필이 너무 광범위하게 정의된 경우 일부 공격이 탐지되지 않을 수 있다. 이로 인해 탐지율이 낮아진다. 반면에, 프로필이 너무 좁게 정의된 경우, 일부 정상적인 활동은 침입으로 탐지될 수 있다. 이로 인해 잘못된 경보가 발생한다. 현재 높은 탐지율과 낮은 거짓 양성률(False-Positive)을 동시에 달성할 수 있는 일반 프로필을 정의하는 효과적인 방법이 없다. 이상 징후 탐지는 침입에 대한 사전 지식이 필요하지 않으며 새로운 침입을 탐지할 수 있지만, 공격이 무엇인지 설명하지 못할 수 있다[4]. 또한, 이상탐지는 정상 행동과 공격 행동이 같은 공간을 공유하고 있으면, 이상치를 식별하기가 어려운데, 이는 결정 경계를 갖는 범위가 매우 불문명하기 때문이다.

우리는 이러한 이상탐지의 한계점에서 알려지지 않는 공격을 식별하기 위한 연구를 수행하였다. 알려지지 않는 공격에서 정상과 유사한 행동을 하는 변종 공격 관점에서 이산 웨이블릿 변환으로 정상과 공격의 행동을 분해하여 재구성을 하고, 정상 공간과 공격 공간간의 비교를 통해 이상치를 식별하는 방법을 수행하였다. 실제 실험으로 우리는 OCSVM(One-Class SVM)을 이용하여 각 클래스마다의 학습을 통해 결정 경계에 있는 이상치를 식별할 수 있었다.

2. 관련 연구

오늘날 사이버 보안의 주요 과제 중 하나는 알려지지 않은 위협을 탐지하는 것이다. 이를 위해 최근 몇 년 동안 많은 연구자들은 탐지율이 높고 거짓 양성률(false positive rate)이 낮은 이상 기반 침입탐지 시스템(Anomaly-based IDSs)을 연구하고 있다. 우리는 알려지지 않는 공격을 탐지하는 사항에 대해 변종을 생성하여 알려지지 않는 방법과 새로운 공격의 유형을 분류하는 방법에 대해 조사하였다.

첫 번째로, 변종을 생성하여 알려지지 않는 유형을 탐지하는 방법으로[5], 이상탐지 영역에서 이상치 탐지(Novelty Detection)는 정상적인 기대치와 일치하지 않는 데이터의 행동을 식별하는 것을 목표로 한다[6]. 이는 단일 클래스 분류(One-Class Classification)이라고도 하지만, 적절한 정상 데이터로 구성된 구축 모델을 통해 정상인지 아니면 새로운지 탐지하는 것을 의미하는데, 정상적인 학습 데이터는 정규성에 대한 설명이 가능한 상태이어야 한다[7]. 즉, 시스템의 정상 상태와 유사하지만, 일치하지 않는 비정상적인 동작을 식별하는 것이다. 이러한 개념을 이용하여 생성 모델을 기반으로 한 방법이 변종 공격으로 알아볼 수 있다. 사이버 보안에서 생성 모델을 이용한 침입 탐지 시스템을 조사하면, 딥러닝(Deep Learning)에서 가장 각광받는 생성적 적대 신경망(Generative Adversarial Network, GAN)과 많이 관련되어 알아 볼 수 있다. 침입탐지 시스템에서 생성적 적대 신경망을 이용한 사항을 확인해보면, 생성 모델에서 학습 데이터의 잡음(noise) 벡터를 생성하여, 판별 모델과 서로 경쟁을 통해 학습하여 변종 공격으로부터 방어를 이루어낸다[8]. 또한 이를 악의적으로 이용한다면 네트워크 데이터에 대한 적대적으로 학습하여 시스템을 파괴하는 방법[9]도 있으며, 이상치 탐지로 접근하기 위해서 학습 데이터의 저밀도 영역의 학습만을 통해 알려지지 않는 공격을 탐지할 수 있다. 이는 균일한 분포에서 쿨백-라이블러(Kullback-Libler) 방법을 이용하여 저밀도 영역

의 변종을 생성함으로써 알려지지 않는 공격에 대한 생성으로 제시될 수 있다[10].

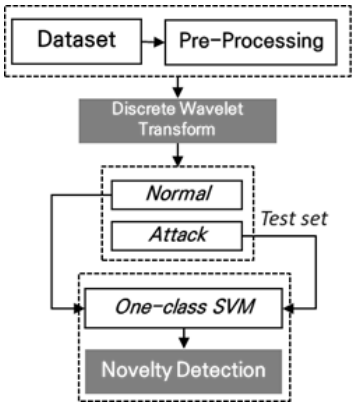
두 번째로, 새로운 공격의 유형을 분류하는 사항에 대해서는 학습모델이 새로운 클래스로 분류하는 것이다. 학습모델은 학습된 클래스에 대해서 정답을 도출해낸다. 이는 학습 공간에 배치되지 않는 데이터도 정해진 클래스에서 정답을 도출하기 때문에 이는 오분류로 나타낼 수 있다. 알려지지 않는 공격의 특성은 앞서 변종과 같이 비슷한 패턴을 보일 수 있지만, 다른 특징 공간을 가질 수 있다. 학습모델에서 이를 해결하기 위한 연구 분야로 Open set recognition[11]이 있으며, 이를 사이버 보안과 같이 알려지지 않는 연구 분야 접목되는 사항도 있다. 해당 방법으로 알려지지 않는 도메인을 찾는 연구 사항에 대해 학습되지 않는 데이터 클래스에 대해 한계점을 극복을 위해 OpenSMax[12]을 제안하기도 하였다. 이는 소프트맥스(Softmax)에 대한 확률 분포를 이용하여 One-Class SVM을 통한 분류로 접목된 사항이다.

우리는 알려지지 않는 공격을 탐지하기 위해서 2가지 유형의 접근법으로 조사하였다. 알려지지 않는 공격을 식별하기 위한 점진적 접근으로, 새로운 클래스로 분류하는 것보다는 학습된 클래스에서 변종의 유형을 찾기 위한 방법을 제안하는 사항을 수행한다.

3. 제안하는 방법

3.1 데이터세트 설명

본 연구에서는 공개적으로 사용 가능한 침입 탐지 데이터세트 NSL-KDD를 사용한다[13]. NSL-KDD 데이터세트는 KDD cup'99의 중복된 레코드를 제거하고, 정제된 버전이다. NSL-KDD 데이터세트의 구성은 학습 레코드 125,973개와 테스트 레코드 22,544개 포함되어 있다. 41개 속성의 명목(nominal variables) 3개, 이진 6개, 32개의 숫자 속성을 포함하고 있으며 정상 활동 및 24개의 공격을 포함한다. 이러한 공격은 네 가지 주요 범주로 DoS, Probe, R2L, U2R로 분류된다. DoS(Denial-of-Service) 공격은 네트워크 액세스를 비활성화하려는 시도에 대한 정보를 갖고 있으며, R2L(Remote-to-Local)은 원격 사용자가 네트워크를 통해 컴퓨팅 시스템으로부터 패킷을 전송하여 로컬 사용자 계정에 대한 액세스 권한을 얻는 것을 나타낸다. 이는 알려진 취약성을 찾기 위한 정보를 수집하는 행위이다. U2R(User to Root)은 공격자가 시스템을 루트 사용자로 탐색하여 일반 사용자의 계정에 액세스함을 나타낸다. 우리의 연구는 학습 데이터와 테스트 데이터를 결합하였으며, 총 148,517개의 입력 데이터로 사용되었다. 이는 U2R 클래스는 분포가 너무 적어 본 실험사항에서는 제외되었다.



(그림 1) 이산 웨이블릿 변환 기반 이상 탐지
(Figure 1) Discrete Wavelet Transform based Anomaly Detection

3.2 전처리 방법

NSL-KDD 데이터세트는 프로토콜 유형, 서비스 및 플래그를 포함하는 3가지 명목 변수가 포함되어 있다. 명목 변수는 많은 고유한 속성 값이 포함되어 있다. 프로토콜 유형에는 세 가지 특성 TCP, UDP, ICMP가 있고, 서비스에는 70개의 속성 값 HTTP, SSH 등 이 포함되어 있으며. flag 속성에는 11개의 특성 SF, S2, S1, S3, 등이 있다. 3가지의 명목 변수를 사용하기 위해 우리는 OneHotEncoder 방식을 적용하였다. 프로토콜 유형의 속성 값이 "TCP"이면 1로 변환되고, 그렇지 않으면 0으로 변환함으로써 각각의 모든 속성을 조합하여 적용하였다. 이를 통해 우리는 77가지의 명목 변수를 생성하였고, 6가지의 이진 속성과 나머지 숫자 속성의 32개를 더해 115개를 생성하였다. 이후, 특성 값이 0인 속성 "wrong_fragment", "urgent", "num_outbound_cmds"을 추가로 제거하여 총 112개의 특성을 사용하여 우리는 다음 단계의 이산 웨이블릿 변환을 수행한다.

3.3 이산 웨이블릿 변환

이산 웨이블릿 변환(Discrete Wavelet Transform, DWT)

은 주어진 신호를 여러 세트로 분해하여 입력 데이터에 숨겨진 패턴을 발견하는 기능을 가지고 있다. 이산 웨이블릿 변환은 입력 데이터를 결정된 수준까지 분해하여 시간-주파수 분석을 위한 기법이다. 입력 데이터를 분해하면 고주파(Detail) 정보의 패턴 변경 등을 나타낼 수 있는데, 이는 데이터로부터의 변형 수준을 관측할 수 있어 네트워크 트래픽과 같은 비정적 데이터를 이해하는 것에 사용될 수 있다[14]. 침입 탐지 시스템에서 대부분의 웨이블릿 변환 기술은 데이터를 재구성하거나 침입 탐지의 임계 값을 결정하는 데 웨이블렛 변환만 사용했다[15].

우리는 본 연구에서 우리는 이산 웨이블릿 변환을 전처리 된 데이터세트에 적용하여, 각 정상과 공격의 각 클래스에 대한 패턴을 이해하고, 클래스간의 균일 분포 속에서 분리될 수 있는 방안으로 적용하였다. 이는 이상 탐지에서 균일 된 분포는 이상치를 탐지하기가 어려운데, 통일된 분포의 이상치는 아웃라이어(Outlier) 경계가 불확실성이 높기 때문이라고 주장하고 있다[16]. 이에 따라 우리는 이산 웨이블릿 변환을 적용하여, 균일 된 분포를 최소하기 위해 사용되었다. 이산 웨이블릿 변환을 적용하기 위해서는 웨이블릿에 따른 패밀리(Family) 적용이 필요하다[17]. 우리는 광범위하게 사용되는 Daubechies의 웨이블릿의 'db2'를 적용하였으며, 3 단계 분해를 적용하였다. 이에 대한 사항은 [14]을 통해 참고 되었다.

3.4 이상탐지를 위한 One-Class SVM

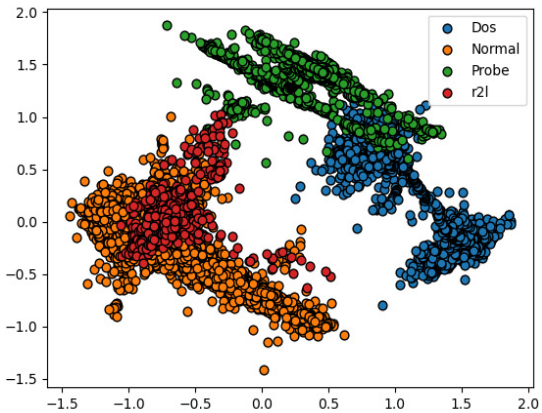
우리는 이상치를 탐지하기 위한 방법으로 결정 경계 추정기의 기반인 OCSVM(One-Class SVM)을 이용한다. OCSVM은 단일 대상 클래스의 패턴만 포함하는 데이터세트를 처리할 수 있다[18]. OCSVM 분류는 대상 샘플의 한 클래스를 다른 모든 클래스와 구별하는 것을 목표로 하며, 이는 주어진 데이터 세트의 대부분의 데이터를 둘러싸는 최소 볼륨 윤곽선을 학습해야 한다. 이러한 특성으로 학습 데이터세트 내의 다른 데이터를 찾는 데 사용되어, 이상치 탐지에 적합하다.

우리는 데이터세트의 각 클래스에 대한 정상의 단일 클래스를 학습하고, 이외 클래스에 대한 특징 공간을 통해 이상치를 판단한다. 학습은 정상 트래픽 데이터만 사용하는 것이 아닌, Normal, Dos, Probe, R2L을 각각 학습하여 각 클래스에 대한 특징 공간 내에 이상치를 식별한다.

4. 실험 결과

4.1 데이터 세트의 이산 웨이블릿 변환 결과

본 연구의 실험 결과 사항으로 전처리된 NSL-KDD 데이터세트의 이산 웨이블릿 변환을 적용하여 특징을 표현한다. 특징 공간을 시각화로 투영하기 위해 우리는 주성분 분석(Principal component analysis) 계산을 수행하여 주요 구성 요소를 식별하였다. 주성분 분석은 고유 벡터와 고유 값을 계산하기 위해서 특이 값 분해(Singular Value Decomposition, SVD)를 기반으로 한 근사 방법을 사용하여, 고차원 데이터를 저차원으로 표현한다.



(그림 2) 이산 웨이블릿 변환과 주성분 분석을 이용한 특징 공간 표현

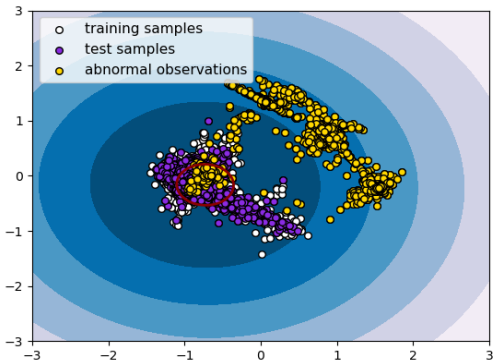
(Figure 2) Feature Space Expression Using Discrete Wavelet Transform and Principal Component Analysis

그림 2는 이산 웨이블릿 변환을 수행하고 주성분 분석으로 두 가지 특징으로 투영된 공간을 나타낸다. 해당 공간에서 4가지 클래스에 대한 범주를 확인해보면, 정상(Normal)으로 표현된 사항은 R2L과 비슷한 공간을 형성하는 것을 확인할 수 있고, DoS 공격은 주로 Probe 공격과 겹치는 공간을 확인할 수 있다. 이는 세 공격 간의 차이를 식별하는 것은 다른 클래스와 유사한 패턴을 유지한다는 사실 때문에 각각의 클래스를 식별하기가 매우 어렵다는 것을 확인할 수 있다. 이는 침입탐지 시스템 문제에서 KDD'99 데이터세트와 같은 도전과제로 많은 연구자들이 이를 식별하기 위해 수행

하고 있다[14][18]. 그리고 이상치를 식별하기 위해서는 균일 된 분포에서는 이상치를 식별하기가 어려운데, 이는 균일 된 분포에서는 결정 경계가 모호하므로[16], 그림 2와 같이 어느 정도 클래스간의 분리가 이루어질 필요가 있다.

4.2 이상탐지 분류 결과

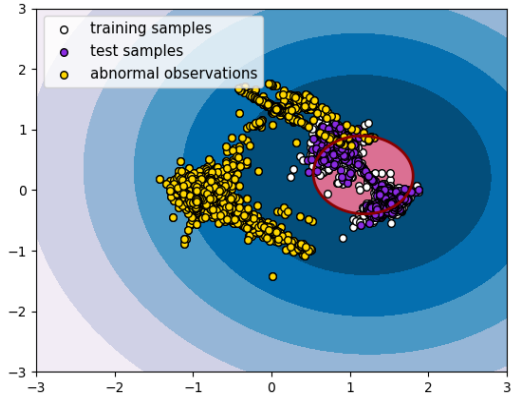
본 실험 결과에서는 이산 웨이블릿으로 분리된 클래스간의 사항에서 이상치를 식별하기 위해 OCSVM을 수행한다. OCSVM은 단일 대상 클래스만을 학습하여 다른 모든 클래스와 구별한다. 우리는 각각의 클래스를 하나씩 학습하여, 학습 결과를 기반으로 다른 클래스에 대한 이상치를 식별하는 방법으로 정상(Normal), DoS, Probe, R2L 클래스를 각각 비교해본다.



(그림 3) 정상(Normal) 클래스 기반 이상 탐지
(Figure 3) Normal Class based Abnormal Detection

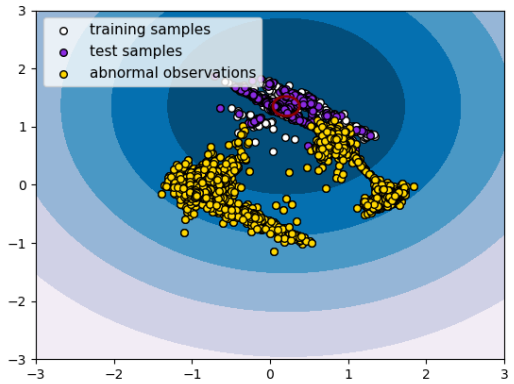
그림 3은 정상(Normal) 클래스를 OCSVM 모델에 학습하고 나머지 클래스를 테스트로 사용된 공간이다. 그림 3에서 알 수 있듯이 하얀색 데이터는 학습데이터이고, 보라색 데이터는 테스트 데이터이며, 노란색 데이터는 이상치를 나타내는 데이터로 표현하였다.

이상치를 나타내는 데이터는 Probe와 DoS 클래스가 명확히 분리되어 이상치를 나타내지만, R2L 클래스의 몇몇 일부는 정상 클래스 공간과 공유된 사항에서 이상치로 식별되는 사항이 있다. 이 부분에 대해서 결정 경계를 갖는 영역 안에 있는 이상치는 정상과 유사한 공격을 나타내는 변종 공격으로 식별될 수 있으며, 이는 우리의 알려지지 않는 공격에 대한 2가지 범위에 변종 공격에 대한 식별로 분류될 수 있다.



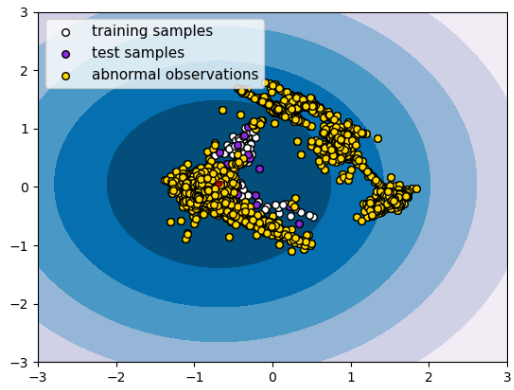
(그림 4) Dos 클래스 기반 이상 탐지
(Figure 4) Dos Class based Abnormal Detection

그림 4에서는 DoS 클래스를 학습하고 나머지 클래스를 테스트로 표현된 공간을 확인할 수 있다. 정상 클래스와 R2L 클래스는 명확히 이상치로 식별되어지지만, Probe 공간과 공유된 결정 경계 안에서 유사한 행동이 있는 알려지지 않는 공격이 있는 것을 확인할 수 있다.



(그림 5) Probe 클래스 기반 이상 탐지
(Figure 5) Probe Class based Abnormal Detection

그림 5에서도 Probe 클래스를 학습하고 나머지 클래스를 테스트로 표현된 공간을 확인한다. 정상 클래스와 R2L 클래스, 그리고 DoS 클래스의 일부만을 명확히 이상치로 식별됨을 확인할 수 있으나, Probe 공간의 공유된 결정 경계 안에서는 다른 클래스의 알려지지 않는 샘플이 없는 것을 확인할 수 있다.



(그림 6) r2l 클래스 기반 이상 탐지
(Figure 3) r2l Class based Abnormal Detection

그림 6에서는 R2L 클래스를 학습하고 나머지 클래스를 테스트 데이터로 표현된 공간을 확인해본다. 정상 클래스와 공유된 사항을 확인할 수 있는데 결정 경계 안에서 몇몇의 데이터가 정상 클래스와의 관계를 알 수 있지만, R2L 데이터 샘플은 매우 적기에 이는 평가가 매우 어렵다. 이는 학습 아래의 표1, 표2로 확인이 가능하다.

(표 1) OCSVM의 학습 성능 평가
(Table 1) Training Data Performance Evaluation

Train Data	Accuracy	Precision	Recall	f1-score
Normal	95.92%	96.24%	96.27%	96.26%
DoS	97.89%	99.76%	94.16%	96.88%
Probe	98.03%	100%	77.03%	87.03%
R2L	97.86%	50.29%	6.84%	12.04%

(표 2) OCSVM의 테스트 성능 평가
(Table 2) Test Data Performance Evaluation

Test Data	Accuracy	Precision	Recall	f1-score
Normal	96.05%	96.24%	96.53%	96.39%
DoS	98.00%	99.69%	94.61%	97.08%
Probe	97.89%	100%	75.55%	86.07%
R2L	97.85%	56.67%	7.85%	13.78%

표 1의 OCSVM의 학습 결과를 분석해 보면 각 클래스에 대한 정확도는 매우 높은 편을 확인할 수 있으나, Probe 및 R2L의 경우 매우 낮은 재현율을 보이고 있다. 이러한 문제는 표 1 학습 성능 평가 및 표 2의 테스트 성능 평가에서 나타나있듯이 적은 데이터를 기반으로 학습이 이루어지고 테스트가 이루어졌다고 확인할 수 있다. R2L의 경우는 데이터 샘플 수가 다른 클래스에 비해 매우 낮은 분포를 지니고 있어, 이를 해결할 수 있는 사항이 필요할 것이다.

5. 결 론

우리는 사이버 보안에서 알려지지 않는 공격을 식별하기 위해 2가지 정의에서 변종 식별을 위한 연구를 수행하였다. 알려지지 않는 공격의 변종 데이터 식별을 위해 우리는 이상치를 탐지한다. 이상치를 탐지하기 위해서는 균일 된 데이터 분포를 이루는 상황에서는 탐지하기가 어려움을 알고, 우리는 이산 웨이블릿 변환을 통하여 각 클래스에 잡음을 제거하여, 명확한 클래스로 재구성하였다. 이후 이상치를 탐지할 수 있는 OCSVM 모델을 통해 각 클래스 별로 결과를 확인해본바, 클래스간의 같은 공간을 공유하고 있는 변종 공격을 식별하였다.

이와 같이 우리는 이상치를 탐지할 수 있는 방법을 제안하였으며, 향후에는 적은 데이터에서도 이상치를 식별할 수 있는 데이터 불균형성을 해결하는 사항을 수행할 것이며, 변종 공격을 생성하는 사항으로 알려지지 않는 공격에 대한 이상치 탐지를 수행할 것이다. 또한 이상치를 탐지하기 위한 여러 모델을 적용하고, 사이버 보안에서 침입탐지 시스템에 적합한 모델을 선별하는 과정을 수행한다.

참고문헌(Reference)

[1] Khraisat. A, Gondal. I, Vamplew. P, and Kamruzzaman. J, "Survey of intrusion detection systems: techniques, datasets and challenges", Cybersecurity, Vol. 2, No. 1, pp. 1-22, 2019. https://doi.org/10.1186/s42400-019-0038-7

[2] Lee. W, Stolfo. S. J, "A framework for constructing features and models for intrusion detection systems", ACM transactions on Information and system security, Vol. 3, No. 4, pp. 227-261, 2000. https://doi.org/10.1145/382912.382914

[3] Sen. J, Mehtab. S, "Machine Learning Applications in Misuse and Anomaly Detection", arXiv preprint arXiv:2009.06709, 2020. http://doi.org/10.5772/intechopen.92653

[4] Narsingyani. D, Kale. O, "Optimizing false positive in anomaly based intrusion detection using Genetic algorithm", 2015 IEEE 3rd International Conference on MOOCs Innovation and Technology in Education, pp. 72-77, 2015.
https://doi.org/10.1109/MITE.2015.7375291

[5] Yamada. A, Miyake. Y, Takemori. K, and Tanaka. T, "Intrusion detection system to detect variant attacks using learning algorithms with automatic generation of training data", Proceedings of International Conference on Information Technology: Coding and Computing, Vol. 1. pp. 650-655 2006.
https://doi.org/10.1109/ITCC.2005.178

[6] Chandola. V, Banerjee. A, Kumar. V, "Anomaly detection: a survey", ACM computing surveys (CSUR), Vol. 41, No. 3, pp. 15-58, 2009.
https://doi.org/10.1145/1541880.1541882

[7] Marco A.F. Pimentel, David A. Clifton, Lei Clifton, and Lionel Tarassenko. "A review of novelty detection. Signal Processing", Vol. 99, pp. 215-249, 2014.
https://doi.org/10.1016/j.sigpro.2013.12.026

[8] Lin, Zilong, Yong Shi, and Zhi Xue, "IDSGAN: Generative adversarial networks for attack generation against intrusion detection." arXiv preprint arXiv:1809.02077, 2018.
https://arxiv.org/abs/1809.02077

[9] Piplai, Aritran, Sai Sree Laya Chukkapalli, and Anupam Joshi, "NAttack! Adversarial Attacks to bypass a GAN based classifier trained to detect Network intrusion." 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). IEEE, 2020.
https://doi.org/10.1109/BigDataSecurity-HPSC-IDS49724.2020.00020

[10] Kliger, Mark, Shachar Fleishman, "Novelty detection with gan", arXiv preprint arXiv:1802.10560, 2018.
https://arxiv.org/abs/1802.10560

[11] Geng, Chuanxing, Sheng-jun Huang, and Songcan Chen, "Recent advances in open set recognition: A survey", IEEE transactions on pattern analysis and machine intelligence, 2020
https://doi.org/10.1109/TPAMI.2020.2981604

[12] Yao Lai, Guolou Ping, Yuexin Wu, Chenhui Lu, and Xiaojun Ye, "OpenSMax: Unknown Domain Generation Algorithm Detection", 24th European Conference on Artificial Intelligence ECAI, Vol. 325, 2020.
http://dx.doi.org/10.3233/FAIA200301

[13] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A Ghorbani, "A detailed analysis of the KDD CUP 99 data set", 2009 IEEE symposium on computational intelligence for security and defense applications, pp. 1-6, 2009.
https://doi.org/10.1109/CISDA.2009.5356528

[14] Ji. Soo Yeon, Jeong. Bong Keun, Choi. Seonho, and Jeong. Dong Hyun, "A multi-level intrusion detection method for abnormal network behaviors", Journal of Network and Computer Applications, Vol. 62 pp. 9-17, 2016.
https://doi.org/10.1016/j.jnca.2015.12.004

[15] TAN Jun, CHEN Xing-shu, DU Min, and ZHU Kai, "A novel internet traffic identification approach using wavelet packet decomposition and neural network", Journal of Central South University, Vol. 19, No. 8, pp. 2218-2230, 2012.
http://doi.org/10.1007/s11771-012-1266-0

[16] Golan, Izhak, Ran El-Yaniv, "Deep anomaly detection using geometric transformations", arXiv preprint arXiv:1805.10917, 2018.
https://arxiv.org/abs/1805.10917

[17] Rashid, Owais, Asdaq Amin, and Mohd Rafi Lone, "Performance Analysis of DWT Families", 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS) IEEE, pp. 1457-1463, 2020.
https://dx.doi.org/10.1109/ICISS49785.2020.9315960

[18] Ritesh K. Malaiya, Donghwoon Kwon, Jinoh Kim, Sang C. Suh, Hyunjoo Kim, and Ikkyun Kim, "An empirical evaluation of deep learning for network anomaly detection", 2018 International Conference on Computing, Networking and Communications (ICNC), pp. 893-898, 2018.
https://doi.org/10.1109/ICCNC.2018.8390278

◐ 저 자 소 개 ◑

김 동 욱 (Dong-Wook Kim)
2015년 가천대학교 컴퓨터공학과(공학사)
2017년 가천대학교 일반대학원 컴퓨터공학과(공학석사)
2017년~현재 가천대학교 컴퓨터공학과 박사과정
관심분야 : Cyber Security, Data Mining, Artificial intelligence
E-mail : kog7306@naver.com

신 건 윤(Gun-Yoon Shin)
2017년 가천대학교 인터랙티브 미디어 융합학과 학사
2018년 가천대학교 일반대학원 컴퓨터공학과(공학석사)
2018년~현재 가천대학교 컴퓨터공학과 박사과정
관심분야 : 기계 학습, 악성코드 분석, 공격자 식별, 저자 분석, 인공지능
E-mail : tlsrjsdbs@gmail.com

윤 지 영(Jiyoung Yun)
2020년 가천대학교 컴퓨터공학과(공학사)
2020년~현재 가천대학교 일반대학원 소프트웨어학과 석사과정
관심분야 : XAI, Machine Learning, Statistics, Intrusion Detection
E-mail : apfhd9043@naver.com

김 상 수(Sang-Soo Kim)
1997년 경북대학교 전자공학과(공학사)
2003년 경북대학교 컴퓨터공학과(공학석사)
2003년~현재 국방과학연구소 연구원
관심분야 : Cyber Security, Cyber Situation Awareness, Artificial Intelligence
E-mail : wisdory@naver.com

한 명 묵(Myung-Mook Han)
1980년 연세대학교 공과대학(공학사)
1987년 뉴욕공과대학교 대학원 컴퓨터공학과(공학석사)
1997년 오사카시립대학교 대학원 정보공학부(이학박사)
1998년~현재 가천대학교 소프트웨어학과 교수
관심분야 : 정보보호, 알고리즘, 데이터 마이닝, 기계 학습
E-mail : mmhan@gachon.ac.kr