KIPS Trans. Softw. and Data Eng.
Vol.12, No.2 pp.99~110
ISSN: 2287-5905 (Print), ISSN: 2734-0503 (Online)

https://doi.org/10.3745/KTSDE.2023.12.2.99

Malicious Traffic Classification Using Mitre ATT&CK and Machine Learning Based on UNSW-NB15 Dataset

Yoon Dong Hyun† · Koo Ja Hwan†† · Won Dong Ho†††

ABSTRACT

This study proposed a classification of malicious network traffic using the cyber threat framework(Mitre ATT&CK) and machine learning to solve the real-time traffic detection problems faced by current security monitoring systems. We applied a network traffic dataset called UNSW-NB15 to the Mitre ATT&CK framework to transform the label and generate the final dataset through rare class processing. After learning several boosting-based ensemble models using the generated final dataset, we demonstrated how these ensemble models classify network traffic using various performance metrics. Based on the F-1 score, we showed that XGBoost with no rare class processing is the best in the multi-class traffic environment. We recognized that machine learning ensemble models through Mitre ATT&CK label conversion and oversampling processing have differences over existing studies, but have limitations due to (1) the inability to match perfectly when converting between existing datasets and Mitre ATT&CK labels and (2) the presence of excessive sparse classes. Nevertheless, Catboost with B-SMOTE achieved the classification accuracy of 0.9526, which is expected to be able to automatically detect normal/abnormal network traffic.

Keywords : Machine Learning, Mitre ATT&CK, UNSW-NB15, Network Traffic Classification, Network Security Monitoring

마이터 어택과 머신러닝을 이용한 UNSW-NB15 데이터셋 기반 유해 트래픽 분류

윤 동 현† · 구 자 환†† · 원 동 호†††

요 약

본 연구는 현 보안 관제 시스템이 직면한 실시간 트래픽 탐지 문제를 해결하기 위해 사이버 위협 프레임워크인 마이터 어택과 머신러닝을 이용하여 유해 네트워크 트래픽을 분류하는 방안을 제안하였다. 마이터 어택 프레임워크에 네트워크 트래픽 데이터셋인 UNSW-NB15를 적용하여 라벨을 변환 후 희소 클래스 처리를 통해 최종 데이터셋을 생성하였다. 생성된 최종 데이터셋을 사용하여 부스팅 기반의 앙상블 모델을 학습시킨 후 이러한 앙상블 모델들이 다양한 성능 측정 지표로 어떻게 네트워크 트래픽을 분류하는지 평가하였다. 그 결과 F-1 스코어를 기준으로 평가하였을 때 희소 클래스 미처리한 XGBoost가 멀티 클래스 트래픽 환경에서 가장 우수함을 보였다. 학습하기 어려운 소수의 공격클래스까지 포함하여 마이터 어택 라벨 변환 및 오버샘플링처리를 통한 머신러닝은 기존 연구 대비 차별점을 가지고 있으나, 기존 데이터셋과 마이터 어택 라벨 간의 변환 시 완벽하게 일치할 수 없는 점과 지나친 희소 클래스 존재로 인한 한계가 있음을 인지하였다. 그럼에도 불구하고 B-SMOTE를 적용한 Catboost는 0.9526의 분류 정확도를 달성하였고 이는 정상/비정상 네트워크 트래픽을 자동으로 탐지할 수 있을 것으로 보인다.

키워드 : 머신러닝, 마이터 어택, UNSW-NB15, 네트워크 트래픽 분류, 네트워크 보안 관제

1. 서 론

네트워크 전문 글로벌기업인 Cisco의 보고에 따르면, 네트워크 트래픽은 2017년 대비 2022년 3배 이상 그리고 매년 4.8ZB 이상 증가할 것으로 추정하고 있다[1]. 이처럼 활발한 네트워킹에 힘입어 인터넷의 의존도가 증가하였고 이에 따라 사이버 공격 발생 시 피해 규모는 더욱 커졌으며, 개인정보 획득, 위조 등의 개인적 피해부터 사이버테러와 같은 국가 차원의 피해까지 피해 범위는 더 넓어졌다. 특히 21세기 인터넷의 발달 이후 국가와 국가 간 혹은 국가와 특정 조직 간에 갈등이 벌어졌을 경우 물리적 공격 수단을 쓰기 이전 사이버 공격 수단을 통해 국가기반망 및 시설을 마비시키는 행위가 동반되고 있다. 최근 우크라이나-러시아 전쟁의 경우 개전 이전, 러시아는 우크라이나 정부, 공공기관 및 금융기관

† 정 회 원 : 성균관대학교 정보보호학과 석사과정
†† 정 회 원 : 성균관대학교 소프트웨어융합대학 초빙교수
††† 종신회원 : 성균관대학교 소프트웨어융합대학 명예교수
Manuscript Received : October 5, 2022
First Revision : November 24, 2022
Accepted : December 14, 2022
* Corresponding Author : Koo Ja Hwan(jhkoo@skku.edu)

등에 대규모 DDoS 발생 및 악성코드를 배포하여 국가적 혼란을 야기했다[2].

이러한 사이버 공격을 방어하기 위해 관·군에서는 법령에 따라 의무적으로 보안 관제센터를 설치 및 운영하여 사이버 공격을 탐지 및 대응하고 있다[3]. 보안 관제센터에서의 주 업무 중 하나는 실시간 네트워크 트래픽을 지속적으로 모니터링 하는 것으로, 비정상 행위가 탐지될 경우 즉각 조치를 취해야 대규모 피해를 방지할 수 있다. 그러나 보안 관제를 수행하는 데 있어 많은 문제점이 발생하고 있으며 다음과 같이 크게 3가지로 분류할 수 있다.

첫째, 시그니처 기반의 현 시스템의 한계이다. 시그니처 기반 탐지 기법의 경우 기존 침해사고 혹은 사이버 인텔리전스로 획득한 URL, HASH, IP 등을 보안장비에 등록하여 필터링을 동작하는 방식으로 위협을 탐지하는데, 알려지지 않은 위협(Zero-Day 등) 및 우회하는 위협에 대한 미탐문제가 발생하고 있다[4, 5].

둘째, 관제 인력 부족이다. 24시간 보안 시스템을 모니터링 해야 하는 관제 인력의 수요 대비 공급이 부족함에 따라 업무 과중화로 피로도가 증가되며 인지력이 감소하는 현상이 발생해 이에 따른 휴먼에러가 우려되고 있다[5].

셋째, 위협 식별 및 분류 단계 시 비표준화·단순분류에 따른 부작용이다. 네트워크 트래픽 모니터링 시, 세부적 분류 없이 단순 정상-비정상으로 바이너리 분류를 하거나 혹은 표준절차 및 표준 표현방식 미적용에 따른 각 관제 인원마다의 주관적인 분류 및 표현 단어 상이함이 발생한다. 이로 인해 의사소통 장애가 발생할 수 있다. 특히 기관·기업의 IT 책임자가 IT·정보보안과 무관한 인원이 담당하는 경우, 침해사고 발생 시 실무자와 의사소통에서 상이한 표현 및 기술적 지식 부족으로 상황 인지시간·대응시간·결심시간이 증가되고 결국 추가 분석 발생 등 후속 조치 지연에 따른 손실이 발생하고 있다[6].

이런 문제점을 해결하기 위해서는 관제 인력 개입을 최소화하기 위한 '인공지능(머신러닝) 기법'을 이용한 자동화 트래픽 분류 시스템을 개발해야 하며, 원활한 의사소통 및 신속한 상황인지를 위한 공신력 있는 표준화된 사이버 위협 프레임워크 적용 방안을 연구할 필요가 있다.

본 연구의 목표는 '네트워크 트래픽'을 표준화된 프레임워크를 통해 표현(라벨)을 변환하고 전처리를 거쳐 이를 머신러닝으로 학습 및 예측하여 실 보안관제에 적용 가능한지에 대한 여부를 확인하는 것이다.

연구는 크게 두 단계로 진행된다. 첫 번째 단계는 네트워크 트래픽 데이터셋을 사이버 보안 프레임워크 중 하나인 마이터 어택(Mitre ATT&CK)[7]에 적용하여 라벨링 작업을 진행할 것이다. 두 번째 단계는 새로운 라벨로 변환된 데이터셋을 사용하여 전처리 작업 후 XGBoost[8], LightGBM[9], Catboost[10] 등과 같은 머신러닝(앙상블)기법을 통해 데이터를 학습시키고 예측하여 결과를 확인할 것이다.

본 연구의 차별성은 크게 두 가지이다. 첫 번째는 최신 네트워크 트래픽의 특성 및 공격 기법을 반영한 데이터셋(UNSW-NB15)[11]에 사이버 보안 프레임워크를 적용하여 새로운 데이터셋을 형성하는 데에 있다. 기존 데이터셋의 경우 네트워크상에서 발생하는 악성 행위를 단순 기술(Technique)로 라벨링을 하였다[11]. 이를 보안 프레임워크를 적용하여 단순기술라벨을 네트워크 침해상황을 고려한 표준화된 악성 행위자의 전술(Tactical)라벨로 변환하였다. 이를 통해 악성행위자의 입장에서 시스템을 대상으로 무슨 목적을 위해 행위를 하는지 확인할 수 있으며, 그리고 방어적인 입장에서 최종적인 목적을 달성하기 위해 후속 악성 행위가 무엇인지 파악 후 대처할 수 있는 방향을 제공한다.

두 번째는 네트워크 데이터셋 내의 희소 클래스를 포함하여 모두 머신러닝에 사용하였다는 점이다. 희소 클래스의 경우 머신러닝 학습 시, 편향성을 불러오기 때문에 기존 연구의 경우 정상-악성으로 바이너리 클래스로 분류하거나 혹은 주요 클래스 일부분만 추출하여 학습하였다[12-15]. 하지만, 본 연구의 경우 희소 클래스 또한 보안관제에 있어서 반드시 관제해야하는 부분이라 판단하여, 샘플링 기법을 사용하여 희소 클래스 문제를 해결하였다.

2. 관련 연구

2.1 인공지능 기반 네트워크 트래픽 분류

인공지능의 연구가 활발해지면서 네트워크 트래픽을 인공지능에 적용하여 네트워크 트래픽 유형 분류를 위한 학습 및 예측하는 연구가 Table 1과 같이 진행되었다.

네트워크 트래픽을 학습하기 위해서는 데이터셋이 필요한데, ISP·통신사 등의 실제 데이터를 사용하는 경우[12]와 가상환경을 구축하여 트래픽을 생산하여 얻은 가상 데이터(Table 2)를 사용하는 경우로 나누어진다.

본 연구에서는 가상 데이터인 UNSW-NB15 데이터셋을 사용할 것이다. UNSW-NB15 데이터셋은 Cyber Range Lab of UNSW Canberra에서 주도하여 제작 및 배포한 데이터셋으로, IXIA PerfectStorm Tool을 이용하여 12개의 트래픽 생성 알고리즘을 통해 만들어진 가상의 네트워크 트래픽 데이터셋이다[11]. 현대의 네트워크 상황과 유사하도록 제작하였으며, 42개의 피처를 가진 정상적인 트래픽과 9가지 비정상 행위 트래픽을 포함한다.

원활한 기계학습을 위해 수집한 데이터셋에 대한 적절한 가공이 필요하다. 특히 네트워크 트래픽 데이터셋의 경우 정상과 비정상 클래스 간의 데이터 개수 비율 분포가 균등하지 않은 불균형한 데이터로 희소 클래스 처리를 포함한 데이터 전처리가 필수적이다. 기존 연구를 살펴보면 차원 축소[17], 언더샘플링[18], 오버샘플링[19-23] 등의 다양한 기법을 이용하였고, 본 연구에서는 오버샘플링 기법을 사용하여 전처리를 진행하였다.

가공된 데이터셋을 학습할 알고리즘을 선정하기 위해서 크게 SVM·K-NN[13, 18] 등의 머신러닝 알고리즘을 활용한 경우와 LSTM[14, 15], GRU·Fast-RNN·Fast-GRNN[15], CNN[16] 등

Table 1. Research Examples Using Network Traffic and AI

No.	Research		
	Dataset	Algorithm	Sampling
1	Intrusion detection system using feature selection with clustering and classification machine learning algorithms on the unsw-nb15 dataset[13]		
	UNSW-NB15	SVM, K-NN	X
2	Intrusion Prediction using Long Short-Term Memory Deep Learning with UNSW-NB15[14]		
	UNSW-NB15	LSTM	X
3	Edge-detect: Edge-centric network intrusion detection using deep neural network[15]		
	UNSW-NB15	LSTM, GRU, Fast-RNN, Fast-GRNN	X
4	A Study of Cyber Attacks and Recent Defense System: DDoS Detection and Applying Deep Learning[16]		
	Real Traffic	CNN	X
5	Malicious traffic detection using ensemble learning based on UNSW-NB15 dataset[17]		
	UNSW-NB15	Logistic Regression, RandomForest	X
6	Classification Performance Improvement of UNSW-NB15 Dataset Based on Feature Selection[18]		
	UNSW-NB15	SVM, K-NN	Undersampling

Table 2. Examples of Virtual Network Traffic Datasets

No.	Dataset	Year	Classes
1	KDD CUP 99	1999	5
2	NSL-KDD	2009	5
3	UNSW-NB15	2017	10
4	CICDS2017	2017	15

신경망 기반의 딥러닝 알고리즘을 활용한 경우가 있다. 본 연구에서는 트래픽 분류 시 사용된 데이터 특성의 중요도를 파악하기 용이한 의사결정나무 기법을 사용하였으며, 이중 과적합 방지에 효과적인 앙상블(부스팅) 알고리즘인 XGBoost[8], LightGBM[9], Catboost[10]를 선정하였다. 보편적인 방법으로 Train 데이터로 학습을 진행하며, Test 데이터를 통해 Validation을 진행하였고, 다양한 측정 지표(F-1 Score, AUC 등)를 통해 결과를 비교하여 적합한 학습 알고리즘 및 희소 클래스 처리기법을 선정하였다.

2.2 사이버 보안 프레임워크

인터넷이 등장한 초기에는 단순 호기심에 따른 개인을 목표로 사이버 내 해커 개인이 주도하는 악성 행위가 주를 이루었지만, 인터넷의 보편적인 사용에 따른 의존도 증가로 사이버 내 악성 행위는 기업·국가를 타깃으로 하여 다양한 목적을 달성하기 위한 공격 조직이 주도하는 APT 공격(지능형 지속 공격)의 빈도가 높아지고 있다.

APT를 수행하는 공격 조직의 경우 (1) 고정적인 공격 타깃 (2) 고정적인 공격 목적 (3) 목적을 달성하기 위한 특정 기법 개발 및 변형 사용의 특징을 가지고 있다. 위 특징을 이용하여 선제적인 방어를 하고자 공격 조직에 대한 TTP(Tactical·Technique·Procedure, 전술·기법·절차)를 분석하였고 이를 표준화·절차화·문서화하고자 사이버 보안 프레임워크가 등장하였다. 대표적으로 미국 방산업체 Lockheed Martin의 Cyber Kill-Chain[24]과 비영리 조직 Mitre의 Mitre ATT&CK[7]가 이에 해당한다. 본 연구에서는 APT 공격 대한 방어 전략을 수립하는데 적합한[25] Mitre ATT&CK 프레임워크를 사용하여 트래픽을 분류할 것이다.

마이터 어택(Mitre ATT&CK)은 미국정부의 지원을 받는 비영리단체 Mitre에서 제작 및 배포한 사이버 보안 프레임워크이다. 실제 데이터를 기반으로, 적대적인 전술·기술을 총망라하였으며, Cyber Kill-Chain의 단순 시계열 공격 묘사의 한계점과 달리 마이터 어택은 공격 패턴을 TTP로 매핑하여 공격자의 행위를 식별해 줄 수 있다는 특징을 가지고 있다[7]. 이는 APT 공격을 분석하는데 효과적으로 평가받고 있다[25]. 마이터 어택 매트릭스는 3가지 요소로 구성되는데, 적의 목표인 전술(Tactics), 전술을 달성하는 방법인 기술(Techniques), 그리고 기술을 구체적으로 이행하기 위한 절차(Procedures)로 구성되어 있다. 마이터 어택 기업용 기준 Table 3과 같이 총 14개의 전술로 구성되어 있다.

본 연구에서는 획득한 데이터셋을 마이터 어택 프레임워크에 적용하여 네트워크 상황과 기술을 고려하여 전술라벨을 생성할 것이다.

2.3 머신러닝 및 부스팅 알고리즘

머신러닝은 인공지능의 분야로, 훈련 데이터(Training Data)의 특성(Feature)을 컴퓨터가 파악하여 학습하고 새로운 데이터가 제시되는 경우 이에 대한 예측을 제시하는 기법이다. 정답지(Labeled Data)를 통해 학습하는 지도학습(Supervised Learning), 정답지 없이(Unlabeled Data) 학습하는 비지도학습(Unsupervised Learning), 그리고 인센티브가 주어지는 시행착오를 통해 인센티브를 최대화하는 행동을 찾아내는 강화학습(Reinforcement Learning)으로 분류할 수 있다.

Table 3. Tactics in Mitre ATT&CK

No.	Tactic	description
1	Reconnaissance	Gather information that can use to plan future operations for adversary
2	Resource Development	Establish resources that can use to support operations for adversary
3	Initial Access	Get into target network
4	Execution	Run malicious code
5	Persistent	Maintain adversary's foothold.
6	Privilege Escalation	Gain higher-level target system's permissions.
7	Defense Evasion	Avoid being detected by target system
8	Credential Access	Steal account names and passwords in target system
9	Discovery	Figure out target environment.
10	Lateral Movement	Move through target enviroment
11	Collection	Gather data of interest to adversary's goal.
12	Command and Control	Communicate with compromised target systems to control them.
13	Exfiltration	Steal target's data
14	Impact	Manipulate, interrupt, or destroy target system and data

본 연구에서는 머신러닝 알고리즘 중 앙상블(Ensemble) 기법을 이용하였다. 앙상블 기법은 머신러닝의 지도학습 방식 중 하나로써 여러 개의 분류기를 생성하고 그 예측을 결합하여 보다 정확하고 신뢰성이 높은 예측값을 도출하는 기법으로, 올바른 예측은 강화하고 잘못된 예측은 상쇄하는 경향을 이용하는 머신러닝 기법 중 하나이다. 정형화된 데이터와 데이터셋의 크기가 크지 않은 경우 딥러닝에 비해 효과적인 성능을 보이는 것으로 알려져 있으며[26], 기법의 대표적인 유형으로는 보팅(Voting), 배깅(Bagging), 부스팅(Boosting) 등이 있다.

본 연구에서는 부스팅 기법을 이용하였다. 부스팅 기법은 앙상블 기법의 하위 기법으로, 여러 개의 예측력이 약한 모형을 순차적으로 결합하여 학습 및 예측을 수행하는 기법이다. 잘못 예측한 데이터에 가중치 부여(Boost)하는 방식으로 진행된다. 타 앙상블 기법에 비해 일반적으로 성능이 우수하나, 학습 속도가 느리고 과적합 가능성이 있다. 대표적인 부스팅 기법은 XGBoost[8], LightGBM[9], Catboost[10] 등이 있다.

3. 실 험

3.1 실험 개요

UNSW-NB15 데이터셋을 이용하여 분석·가공 후, 마이터 어택 프레임워크를 통해 라벨 변환을 진행한다. 이후 희소클래스 처리절차를 거쳐 앙상블(부스팅) 알고리즘을 통해 학습 및 평가하는 방식(Fig. 1)으로 진행될 것이다.

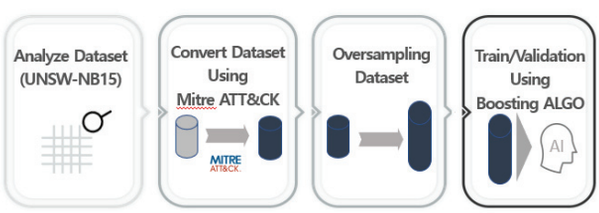


Fig. 1. Research Process

3.2 UNSW-NB15 데이터셋 분석

본 연구에서는 UNSW-NB15 데이터셋을 8:2 비율로 랜덤 추출을 통해 Train/Test 데이터셋을 형성하였다. Train 데이터셋의 개수는 206,138개이며, Test 데이터셋의 경우 51,535개이다. 데이터셋은 42개의 피처를 가지며, 정상적인 트래픽(Normal 클래스)과 9가지 비정상 행위(공격 클래스) 트래픽으로 분류된다.

42개 피처(Table 4)의 경우 가상의 네트워크 환경을 구축하여 유/무해 악성 행위를 네트워크상에 진행하면서 트래픽을 캡처한 패킷 정보와 이를 Argus와 Bro-IDS 툴을 이용하여 분석한 내용을 포함하였다.

Table 4. Features in UNSW-NB15 Dataset

No.	Feature name	No.	Feature name
1	srcip	22	dtcpb
2	sport	23	smeansz
3	dstip	24	dmeansz
4	dsport	25	trans_depth
5	proto	26	res_bdy_len
6	state	27	Sjit
7	dur	28	Djit
8	sbytes	29	Stime
9	dbytes	30	Ltime
10	sttl	31	Sintpkt
11	dttl	32	Dintpkt
12	sloss	33	tcprtt
13	dloss	34	synack
14	service	35	ackdat
15	Sload	36	is_sm_ips_ports
16	Dload	37	ct_state_ttl
17	Spkts	38	ct_flw_http_mthd
18	Dpkts	39	is_ftp_login
19	swin	40	ct_ftp_cmd
20	dwin	41	ct_srv_src
21	stcpb	42	ct_srv_dst

Table 5. Classes in UNSW-NB15 Dataset (Train Set)

No.	Class Name	Number	Ratio
1	Normal	74364	36.07%
2	Generic	47144	22.87%
3	Exploits	35592	17.27%
4	Fuzzers	19398	9.41%
5	DoS	13087	6.35%
6	Reconnaissance	11229	5.45%
7	Analysis	2105	1.02%
8	Backdoor	1858	0.90%
9	Shellcode	1214	0.59%
10	Worms	147	0.07%

비정상 클래스(Table 5)의 경우 IXIA PerfectStorm Tool로 생성하였고, 이를 Backdoor, DoS, Shellcode와 같이 기술적 표현으로 클래스를 명명했다.

Train 데이터셋의 클래스 분포를 확인한 결과, Normal 클래스의 경우 약 36%를 차지하는 반면 Worm 클래스의 경우 0.07%, Shellcode 클래스는 0.59%, Backdoor 클래스는 0.90%, Analysis 클래스는 1.02%를 차지하고 있다. 10개의 클래스 중, 4개의 클래스가 약 1% 이하를 차지하는 상당히 불균형한 데이터셋이며, Table 5와 같이 데이터 불균형을 명확하게 확인할 수 있다. 이는 통상적으로 네트워크 내 보안 시스템(IDS 등)에서 패킷 캡처시, 정상 패킷이 비정상 패킷에 비해 확연히 비율이 높은 현상을 데이터셋에 반영한 것을 확인할 수 있다.

3.3 마이터 어택 프레임워크 적용

UNSW-NB15 데이터셋의 라벨(클래스)을 마이터 어택 프레임워크를 사용하여 마이터 어택 전술라벨로 변환하는 작업을 진행하였다. UNSW-NB15 배포문서 내 라벨별 생성 방법을 바탕으로 변환을 진행하였고, 변환 중 UNSW-NB15 라벨과 마이터 어택 전술라벨이 단수(1:1)연결이 아닌 복수(1:N)로 연결되는 경우가 일부 발생하였다. 이때 복수 후보군을 아래 3가지 기준과 Fig. 2와 같은 처리 방식으로 적용하였다.

① UNSW-NB15의 생성 환경인 웹 환경에 고려
② UNSW-NB15 라벨 설명서에 해당되는 악성 행위 기술(Technique, 마이터 어택 전술단계의 하위집합)을 모두 포함 가능한 마이터 어택 전술로 변환하여 라벨링
③ 마이터 어택 전술(Tactic) 절차상 가장 빠른 순으로 적용. 단, 전술라벨 후보 중 Impact가 포함되어 있으면 Impact 라벨 부여

처리되어 변환된 Final Class 라벨을 기존 데이터셋에 포함하여 최종 데이터셋을 형성한다. 각 변환된 Final Class 라벨과 변환 근거인 Mitre ATT&CK 전술 하부 요소인 기술(Related Techniques)을 Table 6에 표시하였다. 최종 형성된 데이터셋도 불균형한 데이터셋임을 알 수 있으며 Fig. 3으로 확인 시 확연하게 나타난다.

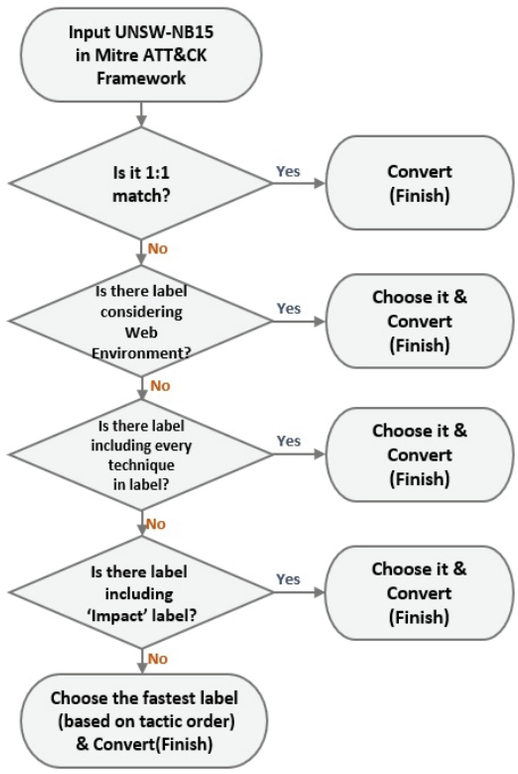
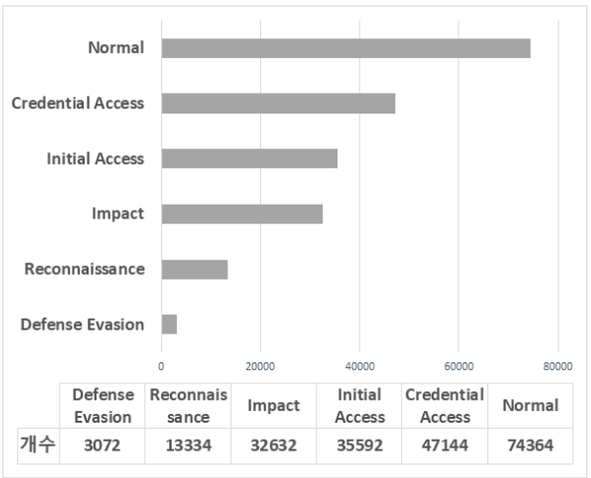


Fig. 2. Flowchart of Conversion Using Mitre ATT&CK Framework

Table 6. Final Converted Classes

No.	Class Name (UNSW-NB15)	Final Class (MItre ATT&CK)
1	Normal	-
2	Analysis	Reconnaissance
	Related Techniques : Active Scanning(Port, Injection for searching Vulnerabilities), Phishing	
3	Backdoor	Defense Evasion
	Related Techniques : Masquerading (Unable to identify security tools by renaming system utilities, deceiving users, and granting services)	
4	DoS	Impact
	Related Techniques : Network·Endpoint Denial of Service, Service Stop by sending big data	
5	Exploits	Initial Access
	Related Techniques : Exploit Public-Facing Application	
6	Fuzzers	Impact
	Related Techniques : System resource exhaustion by sending random and big data	
7	Generic	Credential Access
	Related Techniques : Brute Force	
8	Reconnaissance	Reconnaissance
	Related Techniques : Gather victim host information, Active Scanning	
9	Shellcode	Defense Evasion
	Related Techniques : XSL Script Processing, Exploitation for Defense Evasion	
10	Worms	Impact
	Related Techniques : Data encrypted for Impact, Network Denial of Service, Service Stop	



	Defense Evasion	Reconnaissance	Impact	Initial Access	Credential Access	Normal
개수	3072	13334	32632	35592	47144	74364

Fig. 3. The Number of Classes in Final UNSW-NB15 Dataset

데이터 전처리는 크게 3가지 사항을 진행하였는데, 첫 번째는 불필요한 데이터 특성(Feature)을 제거하는 것이다. UNSW-NB15의 경우 Row의 순서를 기재한 ID값이 이에 해당한다. 두 번째는 결측치를 처리하는 것이다. 결측치 처리 방법의 경우, 데이터 특성의 형식이 수치형 혹은 범주형인지에 따라 처리 방식이 달라진다. UNSW-NB15의 경우, 결측치가 존재하는 특성은 service가 이에 해당한다. service의 경우 범주형이기 때문에 수치형과 같이 평균·최솟값·최댓값 등의 처리가 불가능하기 때문에 결측치에 대해서 NAN 값을 입력하였다. 세 번째는 카테고리 변수를 수치화하는 것이다. 대부분의 머신러닝 분류기의 경우, String으로 표현된 카테고리 변수를 받아들이지 못하기 때문에 이를 수치로 변환하여 표현하였다. 본 연구는 앙상블(부스팅) 알고리즘을 사용하기 때문에 학습 시 영향을 거의 받지 않으므로 저장 공간 낭비를 유발하는 One-hot Encoding 방식보다는 연속적인 수치로 표현하였다. 해당되는 특성은 proto, service, state이다.

3.4 희소 클래스 처리

데이터 학습 편향성을 방지하기 위해 희소 클래스 처리를 진행하였다. Final UNSW-NB15 데이터셋의 경우 Normal 클래스의 경우 전체 데이터셋의 44.9%를 차지하는 반면, Defense Evasion클래스의 경우 1.16%, Reconnaissance 클래스의 경우 5.06%를 차지한다. 불균형한 데이터이기 때문에 그대로 학습하는 경우 편향적 학습가능성이 존재한다. 따라서 오버샘플링·언더샘플링을 통한 Major 클래스와 Minor 클래스 간의 차이를 줄이게 되는데, 본 연구에서는 오버샘플링을 사용하였다.

오버샘플링의 경우 불균형한 데이터셋에서 Minor 클래스의 데이터수를 Major 클래스를 기준으로 수량을 늘려 불균형을 해소하는 방식이다. 언더샘플링의 단점(①학습 데이터 수 감소 ② 분류에 중요한 데이터 배제 가능성 존재)보완이 가능하나, 결국 가상 데이터를 생성 및 기존 데이터셋에 추가하는 과정에서 왜곡이 일어나기 때문에 과적합과 같은 부작용이 존재할 수 있다. 오버샘플링의 경우 데이터셋의 클래스 및 특성의 분포에 따라 적합한 방식이 상이하므로 여러 가지 방법을 사용하여 적합한 방식을 선정하는 것이 적절하다. 본 연구에서는 SMOTE(Sythetic Minority Over-Smapling Technique)[21], Borderline-SMOTE[23] 그리고 ADASYN[22] 방식을 사용하여 비교 분석하였다.

SMOTE의 경우 임의의 Minor 클래스 데이터로부터 인근 Minor 클래스 사이에 새로운 데이터를 생성하는 원리로 진행된다. 수식으로 표현하면 다음과 같다.

$$Synthetic = X + u \bullet (X_n - X) \quad (1)$$

$$Where\ X = Minor\ Class\ Value,$$
$$X_n = X's\ Nearest\ Neighbor,\ u = Random(0<value<1)$$

Borderline-SMOTE의 경우, SMOTE에서 확장한 알고리즘으로 Major클래스와 Minor클래스의 인접 경계에 새로운 데이터를 생성하는 원리로 진행된다. 임의의 Minor클래스의 관측치 X값에 대해 가장 근접한 K개의 데이터를 찾고 3개의 State(아래 참고)로 분류 및 처리한다.

① Danger : X의 근접 데이터 1/2 이하가 Minor 클래스경우, 위험으로 판단하여 SMOTE 적용

② Noise : X의 근접 데이터가 전부 Major 클래스 경우, 노이즈로 판단하여 SMOTE 미적용

③ Safe : X의 근접 데이터가 1/2 초과하는 Minor 클래스 경우, 주변 Minor 클래스가 적절 수준으로 존재하는 것으로 판단하여 SMOTE 미적용

ADASYN(Adaptive Synthetic Sampling Approach)기법은 SMOTE에서 확장한 기법으로, 모든 Minor클래스로부터 동일한 가상 데이터를 생성한 SMOTE와 달리 임의의 Minor클래스의 관측치 X값마다 생성하는 가상 데이터 수가 일정하지 않다. 생성되는 가상 데이터 개수는 관측치 X값의 K-NN(K-Nearest Neighbor) 범위 내로 들어오는 Major클래스 개수에 비례한다.

앞서 전처리가 완료된 데이터셋을 ① 각각의 전술라벨(Multi-Class)와 ② 추후 성능 비교를 위한 정상-비정상라벨(Binary-Class)로 구성하여 회소 클래스 처리하였고, 결과는 Table 7과 같다.

3.5 머신러닝 학습

전처리와 희소 클래스 처리까지 완료된 데이터셋을 바탕으로 머신러닝 학습을 진행하였다. 본 연구에서는 지도학습 방식 중 하나인 앙상블 알고리즘을 선택했으며, 그중 부스팅 계열(XGBoost, LightBGM, Catboost)을 사용하였다. 또한 앙상블 알고리즘의 전반적인 성능 비교를 위해 앙상블 알고리즘의 기본단위(트리)인 의사결정트리(Decision Tree)를 참고용으로 사용하였다. 부스팅 알고리즘 계열의 경우 학습시 주의사항은, 학습 파라미터 조정에 대한 민감성이다. 일반적으로 파라미터 조정에 따른 결과의 변동성이 크기 때문에 최적의 학습 파라미터

Table 7. Classes Distribution (After Preprocessing)

Multi-Class Datasets						
Dataset	Class 0	Class8	Class 3	Class14	Class 1	Class7
X (ORIGIN)	74364	47144	35592	32632	13334	3072
SMOTE	74364	74364	74364	74364	74364	74364
Borderline SMOTE	74364	74364	74364	74364	74364	74364
ADASYN	76817	74672	74382	74364	73725	72046

Class 0 : Normal / Class 8 : Credential Access / Class 3: Initial Access / Class 14 : Impact / Class 1 : Reconnaissance / Class 7 : Defense Evasion

Binary-Class Datasets		
Dataset	Class 0(Normal)	Class 1(Abnormal)
X (ORIGIN)	74364	131774
SMOTE	131774	131774
Borderline SMOTE	131774	131774
ADASYN	132010	131774

Table 8. Optimal Parameters in Each Algorithm

Parameter	Catboost	XGBoost	LightBGM
n_estimator	562	683	504
max_depth	6	10	9
learning_rate	0.25	0.018	0.016

조합 발견이 필수적이다. 이를 해결하기 위해 파라미터 튜닝 자동화 오픈소스인 Optuna 라이브러리[27]를 사용하여 최적의 파라미터를 발견 및 적용하였다. 해당 파라미터는 Table 8과 같다. 이때, 학습에 쓰인 3개의 알고리즘의 공통 파라미터인 n_estimator(생성트리개수), max_depth(트리 최대 깊이), learning_rate(학습률)만 표기하였다.

데이터 분석·머신러닝 학습환경은 아래와 같다.

① 개발언어/에디터: Python 3.8 / Jupyter notebook

② H/W: CPU(Intel Core i7 9750H 2.60 GHz) / GPU(NVIDIA GeForce GTX 1650) / OS(Win 10) / RAM(16GB)

③ 라이브러리: Pandas·Numpy(데이터분석 및 계산), imblearn(샘플링), Optuna(파라미터 자동 튜닝), sklearn (인공지능 지원), xgboost·lightgbm·catboost (머신러닝 알고리즘) 등

4. 성능 평가

4.1 평가 지표

학습모델의 평가 지표로는 혼동행렬(Confusion Matrix)의 구성요소를 조합한 정확도(Accuracy), 정밀도(Prediction), 재현율(Recall), F1-스코어(F-1 score) 그리고 AUC (Area Under the ROC Curve) 등을 적용하였다. 불균형 데이터임을 고려하여 평가 지표 중 정밀도와 재현율의 조화평균인 F1-스코어와 FPR(False Positive Rate)의 변화에 따른 TPR(True Positive Rate)의 변화를 보여주는 ROC(Receiver Operating Characteristic) 곡선의 면적을 계산한 AUC를 중점적으로 비교할 것이다. 혼동행렬(Table 9) 및 지표 계산법. ROC(Fig. 4)와 같다.

Table 9. Confusion Matrix

Confusion Matrix		Prediction	
		Positive	Negative
Result	Positive	True Positive (TP)	False Negative (FN)
	Negative	False Positive (FP)	True Negative (TN)

$$①\text{정밀도}(Precision) = \frac{TP}{TP+FP} \quad (2)$$

$$②\text{재현율}(Recall) = \frac{TP}{TP+FN} \quad (3)$$

$$③\ F1-score = \frac{2\times Precision\times Recall}{Precision+Recall} \quad (4)$$

$$④\ AUC = \int TPR\, d(FPR) \quad (5)$$

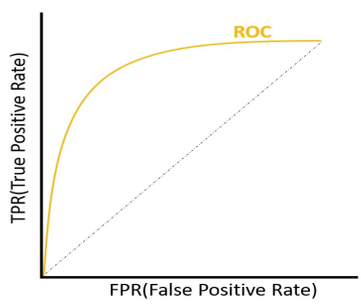


Fig. 4. ROC Curve

이때 F1-스코어를 산출하면서, 데이터셋(ORIGIN)이 불균형 데이터임을 고려하여 전체 Rows 대비 클래스 별 Row 비율에 따른 가중치를 부여 후 계산하였다. 본 연구에서는 오픈라이브러리인 사이킷런(Scikit-learn)의 metric 메소드를 통해 평가지표를 계산하였다.

4.2 평가 결과

① 모든 전술라벨 분류 ② 성능 비교를 위한 정상-비정상 분류 두 가지 케이스로 학습한 머신을 통해 테스트셋으로 평가 한 결과, Table 10, Table 11과 같다.

평가한 내용을 바탕으로 각 머신러닝 기법 별 최고 성능 결과 순위(Top4, F-1 Score 기준) 및 전체 데이터 대상 조합 별 최고 성능 결과 순위(Top4, F-1 Score 기준)를 도출하였고, 각각의 결과(① 전술라벨 분류, ② 정상-비정상 분류)는 Table 12, 13과 같다.

Table 10. Multi-Class Classification Performance Results

Decision Tree(Baseline)					
Dataset	F1 score	AUC	Precision	Recall	Accuracy
ORIGIN	0.7052	**0.9308**	0.6831	**0.7303**	0.7303
SMOTE	**0.7058**	0.9239	**0.8065**	0.6581	0.6581
B-SMOTE	0.6956	0.9295	0.8035	0.6342	0.6342
ADASYN	0.6902	0.9237	0.8008	0.6259	0.6259
Catboost					
Dataset	F1 score	AUC	Precision	Recall	Accuracy
ORIGIN	**0.8142**	**0.9711**	0.8155	**0.8168**	0.8168
SMOTE	0.8022	0.9699	0.8374	0.7797	0.7797
B-SMOTE	0.7987	0.9695	0.8410	0.7720	0.7720
ADASYN	0.7848	0.9681	**0.8509**	0.7450	0.7450
XGBoost					
Dataset	F1 score	AUC	Precision	Recall	Accuracy
ORIGIN	**0.8280**	**0.9741**	0.8383	**0.8266**	0.8266
SMOTE	0.7951	0.9700	**0.8561**	0.7551	0.7551
B-SMOTE	0.7907	0.9691	0.8465	0.7543	0.7543
ADASYN	0.7922	0.9695	0.8532	0.7541	0.7541
LightGBM					
Dataset	F1 score	AUC	Precision	Recall	Accuracy
ORIGIN	**0.7885**	0.9537	0.8250	**0.7764**	0.7764
SMOTE	0.7673	**0.9575**	**0.8438**	0.7260	0.7260
B-SMOTE	0.7550	0.9546	0.8226	0.7241	0.7241
ADASYN	0.7611	0.9548	0.8399	0.7195	0.7195

Table 11. Binary-Class Classification Performance Results

Decision Tree(Baseline)					
Dataset	F1 score	AUC	Precision	Recall	Accuracy
ORIGIN	**0.9248**	0.9038	0.9399	**0.9102**	0.9055
SMOTE	0.9153	**0.9100**	**0.9711**	0.8656	0.8978
B-SMOTE	0.9016	0.8928	0.9579	0.8516	0.8814
ADASYN	0.8925	0.8902	0.9689	0.8273	0.8728
Catboost					
Dataset	F1 score	AUC	Precision	Recall	Accuracy
ORIGIN	0.9433	0.9075	0.9163	**0.9719**	0.9254
SMOTE	0.9525	0.9390	0.9626	0.9426	0.9400
B-SMOTE	**0.9526**	**0.9422**	**0.9695**	0.9364	0.9406
ADASYN	0.9477	0.9262	0.9446	0.9509	0.9330
XGBoost					
Dataset	F1 score	AUC	Precision	Recall	Accuracy
ORIGIN	**0.9503**	0.9186	0.9250	**0.9769**	0.9347
SMOTE	0.9393	0.9385	0.9893	0.8941	0.9262
B-SMOTE	0.9349	0.9355	0.9917	0.8844	0.9213
ADASYN	0.9344	**0.9358**	**0.9933**	0.8822	0.9210
LightGBM					
Dataset	F1 score	AUC	Precision	Recall	Accuracy
ORIGIN	0.9122	0.8415	0.8536	**0.9795**	0.8797
SMOTE	0.9282	0.8830	0.8965	0.9622	0.9049
B-SMOTE	0.9078	0.9131	**0.9936**	0.8356	0.8916
ADASYN	**0.9407**	**0.9219**	0.9485	0.9331	0.9250

Table 12. Ranking Multi-Class Classification Performance Results

Criterion : Best F-1 Score by Machine learning		
No.	Machine learning - Dataset	F-1 Score
1	XGBoost-ORIGIN	**0.8280**
2	Catboost-ORIGIN	**0.8142**
3	LightGBM-ORIGIN	**0.7885**
4	DecisionTree-SMOTE	**0.7058**
Criterion : Best F-1 Score in Total results		
No.	Machine Learning - Dataset	F-1 Score
1	XGBoost-ORIGIN	**0.8280**
2	Catboost-ORIGIN	**0.8142**
3	Catboost-SMOTE	**0.8022**
4	Catboost-BSMOTE	**0.7987**

Table 13. Ranking Binary-Class Classification Performance Results

Criterion : Best F-1 Score by Machine learning		
No.	Machine learning - Dataset	F-1 Score
1	Catboost-BSMOTE	**0.9526**
2	XGBoost-ORIGIN	**0.9503**
3	LightGBM-ADASYN	**0.9407**
4	DecisinoTree-ORIGIN	**0.9248**
Criterion : Best F-1 Score in Total results		
No.	Machine Learning - Dataset	F-1 Score
1	Catboost-BSMOTE	**0.9526**
2	Catboost-SMOTE	**0.9525**
3	XGBoost-ORIGIN	**0.9503**
4	Catboost-ADASYN	**0.9477**

Table 14. Weight Order of Feature Importance

No.	Catboost	XGBoost	LightGBM
1	smean	sbytes	sbytes
2	sbytes	smean	sttl
3	service	sload	smean
4	sttl	dur	service
5	ct_dst_src_ltm	rate	ct_srv_dst
6	ct_srv_dst	sinpkt	dmean
7	ct_dst_ltm	sjit	ct_dst_src_ltm
8	dbytes	djit	proto
9	dmean	dinpkt	dbytes
10	sjit	dmean	dttl

Two or more of the three algorithms corresponding FI: smean, sbytes, service, sttl, ct_dst_src_ltm, ct_srv_dst, dbytes, dmean, sjit

또한 전술라벨 분류 머신러닝 기준, 데이터셋 내 특성이 모델별 트리 내 노드분기에 영향을 많이 끼친(Weight of Feature importance) 10개를 가중치 순서대로 정리하면 Table 14와 같다.

이 중 9가지 특성이 상위 10개 특성 기준 2번 이상 해당됨을 확인하였다. 이는 라벨 분류에 큰 영향을 끼친 특성으로 판단할 수 있으며 특히 패킷의 크기가 라벨 분류에 있어서 중요한 역할을 한 것을 확인하였다. 위 특성에 대한 설명은 아래와 같다.

① smean : 출발지(src)에 의해 전송된 흐름 패킷 크기의 평균
② sbytes : 출발지에서 도착지(dest)로 흐른 패킷의 크기
③ dbytes : 도착지에서 출발지로 흐른 패킷의 크기
④ ct_dst_src_ltm : 서버에서 http 서비스 제공시, 시간 순 100개의 연결에서 동일한 출발지와 도착지 주소의 연결 수
⑤ ct_srv_dst : 서버에서 http 서비스 제공시, 시간 순 100개의 연결에서 동일한 출발지와 동일한 서비스(service)의 연결 수
⑥ dmean : 도착지에 의해 전송된 흐름 패킷 크기의 평균
⑦ service : OSI 응용계층 상 서비스
⑧ sjit : 출발지에서의 패킷 지터(연속 된 두 패킷 간의 지연 차이)
⑨ sttl : 출발지에서 도착지까지의 TTL

4.3 전술라벨(Multi-Class) 분류 결과 분석

전술라벨 분류 기준 평가 결과를 크게 4가지로 분석하면 다음과 같다.

첫째, F-1 스코어를 기준으로 오버샘플링 기법을 쓰지 않은 ORIGIN 데이터셋을 사용하였을 때 성능이 우수하였음을 확인하였다. 이는, 오버샘플링 기법을 사용하는 과정에서, Major 클래스 개수와 Minor 클래스 개수의 지나친 차이로 인해 Minor 클래스의 유사 데이터를 생성하는 과정 왜곡이 일어났음을 확인하였다.

둘째, F-1 스코어를 기준으로 XGBoost-ORIGIN 조합 결과가 우수하였음을 확인하였다. 본 실험에 쓰인 앙상블 알고리즘 중 시기상으로 가장 고전(2016년 출시)적인 기법이지만, 평가결과상 가장 우수하였다. 가장 최신(2017 출시) 기법인 Catboost의 경우 수치형 특성이 많은 데이터 라벨 분류에서 약하다는 통념[28]이 존재하는데, 본 결과에서 XGBoost가 약진함에 따라 어느 정도 수용됨을 확인하였다. 다만, Top4 내 1개 XGBoost 케이스를 제외한 3개의 케이스의 경우 Catboost이기 때문에 통념을 모두 수용하기는 어렵다. 또한 참고지표로 수행된 Decision Tree(0.7058) 대비 모든 앙상블 기법이 상대적으로 우수함을 확인하였다.

셋째, AUC의 경우 모든 데이터셋-모델 조합이 0.9 이상임을 확인하였고 이는 분류기로서 충분한 성능을 내고 있음을 나타낸다. 본 연구에서 최고 AUC는 0.9741, 최저 AUC는 0.9237을 나타내고 있다. AUC의 경우 1에 근접할수록 성능이 좋으며, 0.9 이상의 경우 좋은 분류기로 평가받고 있다.

넷째, 네트워크 패킷의 행위 라벨 분류에 있어서 패킷의 크기가 분류에서 가장 중요하며 이외에 서버에서의 동일 경로 간의 연결수·동일 출발지와 서비스를 가진 연결 수 등 서버에서 제공하는 연결 특성, 지터 등이 중요함을 확인하였다.

4.4 정상-비정상(Binary-Class)트래픽 분류와 성능비교

F-1 스코어를 기준으로 전술라벨분류 성능과 정상-비정상 분류 성능을 비교하면 정상-비정상 트래픽 분류 성능이 우수한 것을 확인하였다. F-1 스코어 기준 정상-비정상 트래픽 분류의 최고성능이 0.9526인 반면, 전술라벨 분류의 경우 0.8280으로 약 0.124 낮은 것으로 확인되었다.

4.5 결과 의의

평가 결과의 의의를 크게 2가지(샘플링 기법, 머신러닝 기법) 관점으로 정리하였다.

첫째, 불균형 데이터의 학습을 위해서는 데이터셋의 특성에 맞는 샘플링 기법을 탐색해야 한다는 점이다. 본 연구에서 사용된 UNSW-NB15의 경우는 샘플링 기법을 미적용한 데이터셋이 가장 적합한 것을 확인하였다. 다만 흥미로운 부분은, 정밀도를 기준으로 원본 데이터에 비해 오버샘플링기법을 적용한 조합이 대부분 높게 측정되었으나 정밀도와 재현율의 차이는 오버샘플링기법을 적용한 조합이 원본 데이터 적용한 조합보다 큰 것으로 측정되었다. 이는 결국 오버샘플링기법의 데이터셋으로 학습한 머신이 평가 결과 오탐(FN) 비율이 높은 것으로 해석이 가능하다. 이는 UNSW-NB15의

경우 전체 Row 대비 0.07% 만을 차지하는 희소 클래스가 있는 등 상당한 불균형 데이터셋으로, 오버샘플링시 Row수가 충분하지 않은 Minor클래스의 가상 데이터를 만드는 과정에서 왜곡이 일어나 학습에 부정적 영향을 준 것으로 추정된다. 특히 비정상 패킷보다 정상 패킷의 비율이 뚜렷하게 높은 네트워크 트래픽 데이터셋에서 중요한 이슈로 보이며, IDS· UTM 등과 같은 네트워크 침해탐지장비의 경우 오탐을 줄이는 것이 가장 중요하기 때문에 학습 시 샘플링기법 사전 탐색은 필수적인 부분으로 확인된다.

둘째, 데이터셋의 특성에 맞는 인공지능(머신러닝 등) 기법을 탐색해야 한다는 점이다. Catboost의 경우 2017년에 배포된 기법으로 타 기법에 비해 최신 기법이며, 자체적으로 데이터셋에 임의의 시계열 부여를 통한 순서형 부스팅(Ordered Boosting) 및 범주형 변수 자동처리 등의 기능 탑재로 고전 기법에 비해 뛰어난 것으로 알려져 있다[10]. 하지만 본 연구의 결과 XGBoost가 더 높은 평가를 받았다. 이는 앞서 평가한 트래픽 분류에서 중요한 역할(노드분기에 많이 사용)을 한 9가지 특성(Table 9 참조) 중 패킷크기, 연결 수, 지터, TTL 등 8가지 특성이 수치형이라는 점에서 원인을 찾을 수 있다. 통상적으로 XGBoost의 수치형 자료에 대한 우수한 성능을 보여주고 있으며, 위 특성을 살려 가상 네트워크 트래픽 데이터인 KDD CUP 99를 분류하는 캐글 경진대회(2015)에서 상위 10개팀 모두 XGBoost를 적용한 사례가 이를 입증한다[8]. 따라서, 학습 이전에 EDA(Exploratory Data Analysis)기법을 통한 데이터셋의 특성을 파악하는 것과, 특성 파악 결과에 따른 알고리즘 기법을 탐색 및 선정하는 것이 중요하다는 점을 보여주고 있다.

5. 결 론

본 논문은 현 네트워크 보안 관제 시스템의 한계를 보완하기 위해 마이터 어택 프레임워크와 머신러닝을 활용한 네트워크 트래픽 분류 모델을 제시하고 UNSW-NB15 데이터 셋을 사용하여 제안 모델의 성능을 검증하였다. 네트워크 트래픽 데이터셋의 단점인 불균형 라벨 문제점을 해소하기 위해 다양한 오버샘플링을 적용하였고, 앙상블(부스팅) 기법을 통해 학습한 결과 오버샘플링을 적용하지 않은 원본 데이터와 이를 학습한 XGBoost 기법이 가장 성능이 좋은 것으로 확인되었고(최대 F1-스코어 : 0.8280), AUC는 모두 0.9 이상으로 나타났다.

다만, 다양한 공격 시나리오를 정확하게 예측하는 전술라벨 분류 모델 적용 방안은 현 네트워크 관제에 바로 실 적용하기에는 성능이 부족할 것으로 판단된다. 따라서 우선적으로 정상-비정상 패킷 분류 방안을 적용 후, 후속 연구를 통해 충분한 성능이 나오면 전술라벨 분류 방안을 적용하는 방향으로 가야 할 것이다. 이를 위해서는 다양한 인공지능 기법을 통한 학습 및 검증을 통한 정확도 향상이 필요하다. 또한 본 연구에 쓰인 데이터셋 이외의 타 네트워크 트래픽 데이터셋과 실제 네트워크 트래픽 데이터, 침해 사고 데이터 등을 활용하여 상황에 정확히 일치한 마이터 어택 라벨을 부여한 데이터셋을 형성 및 활용하여야 본 연구의 한계점을 극복할 것으로 판단된다. 더불어, 탐지 성능을 높여 SIEM, SOAR와 같은 빅데이터 기반 보안 시스템에 적용[29]하는 방안을 연구한다면 현 네트워크 보안 관제의 문제점을 보완할 것으로 기대한다.

References

[1] Cisco, Visual Networking Index: Global Mobile Data Traffic Forecast Update 2017-2022 [Internet], https://www.cisco.com/c/dam/global/ko_kr/solutions/service-provider/visual-networking-index-vni/.

[2] The institute of Foreign Affairs and National Security(ROK Gov), Cyberwarfare in the Russo-Ukraine War: Evaluation and Implications [Internet], https://www.ifans.go.kr/.

[3] National Intelligence service Republic of Korea, Operational Rules for Cybersecurity (Goverment Rule) [Internet], https://www.law.go.kr/.

[4] H. Hwang, D. Moon, and I. Kim, "Trend and issue dynamic analysis for malware," in *Proceedings of the Korea Information Processing Society Conference*, *The KIPS*, pp.418-420, 2015.

[5] J. W. Ji, "Problems of cyber security control system and the application of machine learning technology," *Review of Korea Institue of Information Security and Cryptology*, Vol.31, No.3, pp.13-19, 2021.

[6] K. H. Kim, K. D. Park, and M. N Sim, "A study on the organizational conflict and job withdrawal intention of the information security workers," *Journal of the Korea Institute of Information Security & Cryptology*, Vol.29, No.2, pp.451-463, 2019.

[7] Mitre, Mitre ATT&CK [Internet], https://attack.mitre.org.

[8] T. Chen and C. Guestrin. "Xgboost: A scalable tree boosting system," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ACM SIGKDD, 2016, pp.785-794.

[9] G. Ke et al., "Lightgbm: A highly efficient gradient boosting decision tree," in *Advances in Neural Information Processing Systems*, 30, NIPS, 2017.

[10] A. V. Dorogush, V. Ershov, and A. Gulin, "CatBoost: gradient boosting with categorical features support." *arXiv preprint arXiv:1810.11363*.

[11] M. Nour and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *2015 Military Communications and Information Systems Conference (MilCIS)*, IEEE, 2015, pp.1-6.

[12] I. H. Seok, K. T. Lee, J. H. Yu, and S. J. Kim, "CNN based Real-Time DNS DDoS attack detection system," *The KIPS Transactions on Computer and Communication Systems*, Vol.6, No.3, pp.135-142, 2017.

[13] M. Hammad, W. El-medany, and Y. Ismail, "Intrusion detection system using feature selection with clustering and classification machine learning algorithms on the unsw-nb15 dataset," in *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)*, IEEE, pp.1-6, 2020.

[14] S. S. Kim, L. Chen, and J. Y. Kim, "Intrusion prediction using long short-term memory deep learning with UNSW-NB15," in *2021 IEEE/ACIS 6th International Conference on Big Data, Cloud Computing, and Data Science (BCD)*, IEEE, 2021.

[15] P. Singh, J. Jaykumar, A. Pankaj, and R. Mitra "Edge-detect: Edge-centric network intrusion detection using deep neural network," in *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, IEEE, 2021.

[16] Y. H. Lee, S. H. Baek, J. W. Seo, I. Y. Bang, and Y. H. Paek, "A study of cyber attacks and recent defense system: DDoS detection and applying deep learning," in *Proceedings of the Korea Information Processing Society Conference*, The KIPS, pp.302-305, 2017.

[17] P. D. Yoon and K. H. Hwang, "Malicious traffic detection using ensemble learning based on UNSW-NB15 dataset," in *2021 KICS Winter Conference*, KICS, 2021.

[18] D. B. Lee and J. H. Seo, "Classification performance improvement of UNSW-NB15 dataset based on feature selection," *Journal of the Korea Convergence Society*, Vol. 10, No.5, pp.35-42, 2019.

[19] R. Malhotra and S. Kamal, "An empirical study to investigate oversampling methods for improving software defect prediction using imbalanced data," *Neurocomputing*, Vol.343, pp.120-140, 2019.

[20] R. Mohammed, J. Rawashdeh, and M. Abdullah, "Machine learning with oversampling and undersampling techniques: Overview study and experimental results," in *2020 11th International Conference on Information and Communication Systems (ICICS)*, IEEE, 2020, pp.243-248.

[21] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: Synthetic minority over-sampling technique," *Journal of Artificial Intelligence Research*, Vol.16, pp.321-357, 2002.

[22] H. He, Y. Bai, E. A. Garcia, and S. Li, "ADASYN: Adaptive synthetic sampling approach for imbalanced learning," in *2008 IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence)*, IEEE, pp.1322-1328, 2008.

[23] H. Han, W. Y Wang, and B. H. Mao, "Borderline-SMOTE: A new over-sampling method in imbalanced data sets learning," in *International Conference on Intelligent Computing*. Springer, 2005.

[24] Lockheedmartine, Cyber Kill Chain [Internet], https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-ki-chain.html.

[25] Y. I. Yoon, J. H. Kim, J. Y. Lee, S. D. Yu, and S. J. Lee, "A research on cyber kill chain and TTP by APT attack case study," *Jouranl of Information and Security*, Vol.20, No.4, pp91-101, 2020.

[26] J. Wang, B. Hu, X. Li, and Z. Yang, "GTC forest: An ensemble method for network structured data classification," in *2018 14th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN)*, IEEE, pp.81-85, 2018.

[27] T. Akiba, S. Sano, T. Yanase, T. Ohta, and M. Koyama, "Optuna: A next-generation hyperparameter optimization framework," in *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, ACM SIGKDD, pp2623-2631, 2019.

[28] E. Al Daoud, "Comparison between XGBoost, LightGBM and CatBoost using a home credit dataset," *International Journal of Computer and Information Engineering*, Vol.13, No.1, pp.6-10, 2019.

[29] J. H. Hong and B. Y. Lee, "Artificial intelligence-based security control construction and countermeasures," *Journal of the Korea Contents Association*, Vol.21, No.1, pp.531-540, 2021.

윤 동 현

https://orcid.org/0000-0001-9773-5019
e-mail : lg49oksk@hotmail.com
2019년 공군사관학교 전산과학과(학사)
2019년 ~ 현 재 국방부(공군) 장교
2020년 ~ 현 재 성균관대학교
정보보호학과 석사과정
관심분야 : Cyber Threat Analysis, AI(Pattern Recognition), Data Mining

구 자 환

https://orcid.org/0000-0002-2844-3183
e-mail : jhkoo@skku.edu
1995년 성균관대학교 정보공학과(학사)
1997년 성균관대학교 전기전자컴퓨터공학과 (석사)
1999년 ~ 2002년 LG CNS 연구원
2006년 성균관대학교 전기전자컴퓨터공학과(박사)
2007년 ~ 2010년 미국 위스콘신대학교 컴퓨터과학과 박사후 연구원
2019년 ~ 현 재 성균관대학교 소프트웨어융합대학 초빙교수
관심분야 : Data Communication, Computer Network, Big Data, Machine Learning, Data Security

원 동 호

https://orcid.org/0000-0002-5208-1338
e-mail : dhwon@security.re.kr
1976년 성균관대학교 전자공학과(학사)
1978년 성균관대학교 전자공학과(석사)
1988년 성균관대학교 전자공학과(박사)
1978년 ~ 1980년 한국전자통신연구원 전임연구원
1985년 ~ 1986년 일본 동경공업대학교 객원연구원
2002년 ~ 2003년 한국정보보호학회장
1982년 ~ 2015년 성균관대학교 컴퓨터공학과 교수
2015년 ~ 현 재 성균관대학교 소프트웨어융합대학 명예 교수
관심분야 : Cryptography, Authentication Scheme, Security Algorithms