AutoEncoder-XGBoost 기반 경량 하이브리드 네트워크 침입 탐지 방법

김범수, 최원석*
충북대학교
bmori3@naver.com, *wschoi@cbnu.ac.kr

Lightweight AutoEncoder-XGBoost-Based Hybrid Network Intrusion Detection Method

Kim Beom Su, Choi Won Seok
Chungbuk National Univ.

요 약

본 논문은 AutoEncoder와 XGBoost 기반의 경량 하이브리드 네트워크 침입 탐지 방법을 제안한다. 인공지능을 활용하여 네트워크 침입 탐지를 수행하기 위해 하이브리드 형태로 인공지능 모델을 제안하는 연구가 활발히 진행되고 있다. 기존 연구는 탐지율 향상을 위해 새로운 알고리즘 추가와 모델의 변경을 수행하고 이에 따른 학습 및 추론 자원을 요구한다. 하지만, 스마트폰 및 개인 PC 등과 같은 하드웨어 성능이 제안되는 환경에서는 기존 연구의 높은 자원 요구를 만족시키기 어렵다. 따라서, 본 논문에서는 복잡한 추가 모듈 없이 단일 AutoEncoder와 XGBoost의 경량화된 파이프라인을 통해 학습 및 추론 시 요구되는 높은 메모리 및 연산 요구량 없이 자원이 제한된 환경에서 빠르게 네트워크 침입 탐지를 수행할 수 있는 시스템을 제안하고 실험을 통해 제한된 자원 환경에서도 높은 검출률과 활용 가능성을 확인하였다.

Ⅰ. 서 론

최근 인공지능, 자율주행, IoT 등 다양한 기술들이 정보통신 기술과 융합하여 발전하고 있다. 다양한 정보통신 융합 기술의 발전과 함께 지능형 사이버 공격도 고도화되면서, 침입 탐지 시스템은 네트워크 보안의 필수 요소로 자리 잡고 있다. 특히 최근에는 머신러닝 및 딥러닝 기반의 인공지능 기법을 활용하여 이상 행위를 학습 및 탐지하려는 연구가 활발히 진행되고 있다.[1]

인공지능 기반의 네트워크 침입 탐지 방법은 알려진 공격 패턴 뿐 아니라 새로운 유형의 공격에도 대응할 수 있다는 장점이 있어, 네트워크 보안 분야에서 큰 주목을 받고 있다.[2]-[4]

XIDINTFL-VAE 연구는 클래스별 Focal Loss를 적용한 Variational AutoEncoder로 희소 클래스의 데이터를 합성하여 학습 데이터 분포를 균형화한 뒤, XGBoost 분류기를 사용해 침입을 탐지한다.[2] Logarithmic Autoencoder과 XGBoost 기반 침입 탐지 시스템 연구는 로그 변환 계층을 이용해 데이터 정규화 과정을 대체하고, AutoEncoder로 특징을 추출한 뒤 XGBoost로 분류하는 구조를 제안한다.[3] Kang 등의 AutoEncoder와 XGBoost 기반 침입 탐지 모델 연구는 데이터 불균형 문제를 해소하기 위해 정상 샘플을 업샘플링하고, 랜덤포레스트로 주요 특징을 선별한 뒤 Affinity propagation 알고리즘으로 특징을 그룹화하는 전처리 파이프라인을 제안한다.[4] 하지만, 기존 연구는 탐지율 향상을 위해 새로운 알고리즘 추가와 모델의 변경을 통해 모델의 복잡도를 증가시키고 학습 및 추론 시 높은 메모리와 연산 자원을 요구한다. 이는 스마트폰·개인 PC 등 제약된 하드웨어 환경에서는 실제 적용이 어렵게 한다.

따라서, 본 논문에서는 단일 AutoEncoder와 XGBoost로 구성된 경량 하이브리드 파이프라인을 제안한다. 최소한의 메모리 및 연산 자원만으로 학습 및 추론을 수행할 수 있으며, 실험을 통해 제한된 자원 환경에서도 높은 검출률을 달성함을 보인다.

Ⅱ. 본론

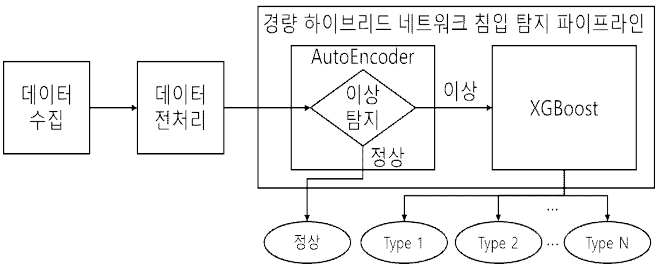

그림 1. AutoEncoder와 XGBoost 기반 경량 하이브리드 네트워크 침입 탐지 시스템

본 논문은 AutoEncoder와 XGBoost 기반의 경량 하이브리드 네트워크 침입 탐지 방법을 제안한다. 그림 1은 본 논문에서 제안하는 경량 하이브리드 네트워크 침입탐지 시스템을 보여준다. 데이터가 수집되면 데이터 전처리를 수행하고 AutoEncoder와 XGBoost로 구성된 경량 하이브리드 네트워크 침입 탐지 파이프라인을 통해 이상 행위 패킷 여부와 타입을 분석한다. 데이터 수집은 학습 상황에서의 학습 데이터셋이며, 추론 상황에서 유입된 패킷이다. 데이터 전처리는 데이터 학습 및 추론을 위해 범주형 변수 원핫 인코딩과 연속형 변수 정규화를 수행한다. 데이터 학습시 정상/비정상 데이터 분할도 수행한다. 경량 하이브리드 네트워크 침입 탐지 파이프라인은 AutoEncoder와 XGBoost로 구성된다. AutoEncoder를 통해 정상 패턴 학습을 수행하고 잠재 공간을 표현하여 재구성 오차를 계산한다. XGBoost는 이상 행위 패킷에 대해 특성 중요도를 분석한다. 추론시, AutoEncoder는 임계값 기반으로 이상 행위 패킷 탐지를 수행하고 이상행위 패킷으로 추론되면 XGBoost를 통해 이상 패킷 유형을 DoS, Probe, R2L, U2R 등과 같이 다중 클래스를 분류한다.

Ⅲ. 실험

본 절에서는 제안하는 AutoEncoder 와 XGBoost 기반 경량 하이브리드 네트워크 침입 탐지 방법을 KDD99 데이터셋을 기반으로 PC 급 하드웨어 환경에서 실험하고 성능을 분석한다.

표 1. 실험 환경

Component		Specification
Hardware	CPU	Ryzen 5900x 3.7GHz
	GPU	NVIDIA RTX 3090
	RAM	DDR4 48GB
Software	Python	3.10
	TensorFlow	2.12.0
	XGBoost	1.7.5

표 1은 실험에서 사용한 하드웨어와 소프트웨어 스펙을 보여 준다. 주요 하드웨어 요소로 CPU는 Ryzen 5900x를 사용했으며, GPU는 NVIDIA RTX 3090을 사용하고 48GB RAM을 사용하였다. 소프트웨어 요소로는 파이썬 3.10 버전을 사용했으면, TensorFlow 2.12.0과 XGBoost 1.7.5 라이브러리를 사용하였다.

표 2. 학습 데이터셋

클래스		데이터셋 수
Normal data		680,805
Abnormal Data	DoS	2,718,505
	Probe	28,759
	R2L	797
	U2R	35
Total		3,428,901

표 2는 학습에 사용한 KDD99 데이터 셋의 클래스와 각 클래스별 데이터셋 수량을 보여준다. 정상 데이터는 680,805개가 사용됐으며, 비정상 데이터는 DoS, Prob, R2L, U2R 공격 데이터를 포함하여 2,748,096개를 사용하였다. R2L과 U2R 공격 데이터는 상대적으로 적은 샘플을 가지고 있다.

표 3은 제안하는 AutoEncoder 와 XGBoost 기반 경량 하이브리드 네트워크 침입 탐지 방법을 KDD99 데이터셋 기반으로 PC 급 하드웨어 환경에서 실험한 클래스별 성능 결과를 보여준다. 이상행위 패킷에 대한 클래스는 DoS, Probe, R2L, U2R 공격 유형으로 분류했으며, 이상행위 패킷과 정상 패킷에 대해 Precision, Recall, F1-score, Support를 측정하였다.

Precision은 Positive 판단의 정확도, 즉 Positive로 추론한 결과 중에 실제 Positive인 정도를 의미하고, Recall은 실제 Positive 패킷에 대해 정확하게 Positive로 추론한 정도를 의미한다. F1-score는 Precision과 Recall의 조화평균으로 두 지표를 균형 있게 평가한다. Support는 샘플 수를 의미한다.

DoS 공격은 전체 샘플 중 제일 많은 부분을 차지하고 있으며, Precision, Recall, F1-score가 1.00로 높은 탐지율을 보였다. Probe 공격은 DoS 공격에 비해 샘플 수가 비교적 적음에도 불고하고 Precision 0.92, Recall 0.94의 높은 성능을 보였고, F1-score는 0.93을 보였다. 하지만, R2L 공격은 샘플 수가 329건으로 Precision 0.06, Recall 0.16, F1-스코어 0.08의 낮은 탐지 성능을 보였다. 또한, U2R 공격은 샘플 수가 17건으로 Recall은 0.76으로 상대적으로 높으나 Precision은 0.11으로 오탐이 많고 F1-스코어는 0.20를 보였다. 마지막으로 정상 패킷은 Precision과 Recall이 모두 0.99로, 모델이 정상과 비정상을 거의 완벽하게 구분하고 있음을 보여준다.

Ⅲ. 결론

본 논문에서는 AutoEncoder와 XGBoost 기반의 경량 하이브리드 네트워크 침입 탐지 방법 제안하고 KDD99 데이터셋을 기반으로 PC 급 하드웨어 환경에서 실험 및 성능 분석을 수행하였다. 실험 결과, 데이터 셋이 많거나 특성이 뚜렷한 공격은 잘 잡아내지만, 샘플 수가 적고 특징이 미묘한 R2L, U2R 같은 클래스에 대해서는 추가적인 데이터 보강이나 인공지능 모델 개선의 필요성이 확인된다.

향후 연구에서는 데이터 보강을 통한 R2L, USR 클래스에 대한 성능 향상 방법 및 기존 연구 대비 자원 이용율 분석을 진행할 예정이다.

ACKNOWLEDGMENT

이 논문은 2025년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. RS-2020-NR049604). 또한, 2025년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No. RS-2024-00397979, 6G 수십 테라급 초정밀 전달망 시스템 기술 개발).

*교신저자: 최원석(wschoi@cbnu.ac.kr)

참 고 문 헌

[1] Truong, T. M., Choi, W. S., Hyeon, J. J., Choi, S. G. “The Development of a New System for Generating Training Data of AI-Based Anomaly Detection,” In 2024 26th International Conference on Advanced Communications Technology (ICACT), Feb. 2024.

[2] Abdulganiyu O. H., Ait Tchakoucht T., Saheed Y. K., Ahmed H. A. “XIDINTFL-VAE: XGBoost-based intrusion detection of imbalance network traffic via class-wise focal loss variational autoencoder,” The Journal of Supercomputing, vol. 81, 2025.

[3] Xu W., Fan Y. “Intrusion Detection Systems Based on Logarithmic Autoencoder and XGBoost,” Security and Communication Networks, vol. 2022.

[4] Kang Y., Tan M., Lin D., Zhao Z. “Intrusion Detection Model Based on Autoencoder and XGBoost,” Journal of Physics: Conference Series, vol. 2171, 2022.

표 3. 클래스별 성능 결과

Class	Precision	Recall	F1-score	Support
DoS	1.00	1.00	1.00	1,164,865
Probe	0.92	0.94	0.93	12,343
R2L	0.06	0.16	0.08	329
U2R	0.11	0.76	0.20	17
Normal	0.99	0.99	0.99	291,976