AutoEncoder 기반 트래픽 분류 기술 최신 동향

서주형[1], 김가영, 김태윤, 배기태, 김찬형[2], 이브라히모바-나일라, 윤종희
영남대학교 컴퓨터공학과 학부생[1], 석사과정[2], 교수[3]
blane7777@naver.com, im_770@naver.com, elma9810@yu.ac.kr, bgt010@naver.com,
qhfrha@yu.ac.kr, 22446177@yu.ac.kr, youn@yu.ac.kr

Recent Trends in AutoEncoder-Based Traffic Classification

Ju-Hyeong Seo[1], Ga-Young Kim, Tae-Yun Kim, Gi-Tae Bae,
Chan-Hyung Kim[2], IbrahiMova-Naila, Jong-Hee Youn[3]
Dept. of Computer Engineering, Yeongnam University

요 약

본 연구는 최근 인터넷 환경에서 암호화 프로토콜의 사용 증가로 기존 방식의 네트워크 트래픽 분류가 제한됨에 따라, 이를 해결하기 위한 오토인코더 기반 트래픽 분류 기법을 분석하였다. Flow Spectrum 및 AMAE 기법은 높은 정확도를 보였으나, 스펙트럼 중첩 현상 및 데이터 편향 문제가 존재했다. Masked AutoEncoder를 적용한 YaTC는 비라벨 데이터를 이용한 사전학습을 통해 정확도와 실용성을 개선하였으나, MFR 형식의 일반화 가능성에 대해 추가 검증이 필요하다.

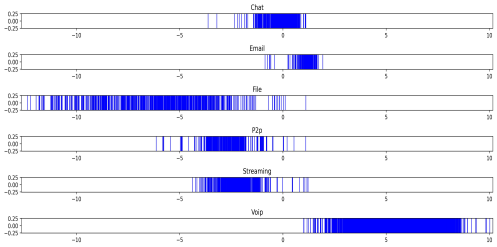
1. 서론

최근 인터넷 트래픽 환경에서 HTTPS 같은 암호화 프로토콜을 사용하는 서비스가 급증함에 따라 패킷 내부 정보를 직접 분석하는 데에 어려움을 겪고 있다.. 유튜브나 넷플릭스와 같은 스트리밍 플랫폼뿐만 아니라 일반 웹 서핑도 암호화를 기본으로 채택하면서 전통적인 포트 기반 분류나 단순 통계 분석만으로는 트래픽 유형을 정밀하게 식별하는 것이 제한되고 있다. 또한, 정상적인 행위의 트래픽과 악의적인 행위의 트래픽이 동일한 암호화 터널을 통해 섞여 지나가는 상황에서, 이를 모니터링하고 분리해 내는 일은 보안 관점에서 점점 더 까다로운 과제로 부각되고 있다.

본 논문에서는 이러한 문제를 해결하기 위한 방안으로 오토인코더(Autoencoder)를 활용한 트래픽 분류기법들을 조사 및 분석하여 기술 동향을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 AutoEncoder를 기반 연구 동향에 대하여 설명하고, 3장에서는 결론을 기술한다.

2. 본론



(그림 1) FlowSpectrum 구조

Cui et al. [1]은 Self-Attention 기법과 Flow Spectrum [2] 이론을 결합한 AMAE(Attention-based AutoEncoder) 모델을 제안하였다. 그림 1은 ISCX-VPN2016 데이터셋에서 추출한 것으로 FlowSpectrum의 구조를 확인할 수 있다. 본 모델은 Sanghyun et al. [3]에서 제안한 Single-Channel Attention 모듈과 Global Spatial Attention 모듈을 각각 Query와 Key로 활용함으로써, 기존 Self-Attention 구조를 개선하였다. Single-Channel Attention은 평균 및 최대 풀링을 통해 채널 차원의 중요 정보를 추출하며, Spatial Attention은 입력의 공간 구조를 보존하여 지역적 중요도 정보를 학습한다. 두 Attention 모듈의 결과는 통합되어 Autoencoder의 입력으로 사용되며, 이는 트래픽 데이터의 전역적·지역적 특징을 동시에

학습할 수 있도록 한다.

AMAE 모델은 ISCX-VPN2016 데이터셋을 기반으로 한 실험에서, 비암호화 트래픽은 100%, 암호화 트래픽은 99.69%의 정확도를 달성하며 기존 AtuoEncoder 기반 모델보다 우수한 분류 성능을 입증하였다. 또한 주의 가중치 시각화를 통해 트래픽 유형별로 스펙트럼 선의 분포 차이를 해석 가능하게 했으며, 다양한 트래픽 유형이 어느 바이트 영역에 주의를 집중하는지 분석할 수 있게 하였다.

Zhao et al. [4]은 Masked AutoEncoder 기반의 사전학습 기법을 활용한 자기지도학습 모델인 YaTC (Yet Another Traffic Classifier)를 제안하였다. 이 모델은 대규모 비라벨 데이터를 활용하여 사전학습을 수행함으로써 라벨 데이터에 대한 의존도를 줄인다. 또한, YaTC는 독자적인 Attention 메커니즘을 적용하기 위해 MFR(Multi-level Flow Representation) 데이터 형식을 고안하였으며, 이를 기반으로 사전학습 단계에서는 Masked AutoEncoder 방식으로 입력을 마스킹하고 복원하는 과정을 반복하여 손실을 계산해, 인코더 가중치를 갱신한다. 미세조정 단계에서는 사전학습된 인코더를 전이하여 패킷 단위와 플로우 단위의 Self-Attention을 순차적으로 적용함으로써 암호화 트래픽 분류를 수행한다. YaTC는 ISCXVPN2016 데이터셋에서 98.07%의 분류 정확도를 기록하였으며, 이는 기존 CNN 기반 모델은 물론 PERT 및 ET-BERT와 같은 최신 모델 대비 10% 이상 높은 성능을 나타낸다. 또한, 비라벨 데이터 기반의 사전학습을 통해 라벨링 비용을 절감하고 데이터 전처리 부담을 완화할 수 있다는 장점을 지닌다.

3. 결론

Cui et al. [1]는 기존 Flow Spectrum에 Self-Attention 기법을 추가하여 더 높은 정확도를 달성하였다. 하지만 스펙트럼 선의 물리적 의미가 불명확성, 스펙트럼 분포 간 중첩 현상 문제가 있었으며 5-tuple과 데이터들이 그대로 포함되어 있어서 편향적 결과가 나올 수 있다는 한계도 존재했다. 그럼에도 Flow Spectrum 방식은 약 95% 이상의 높은 정확도를 보여 활용 가능성이 크며, 한계를 보완할 후속 연구가 필요하다.

Zhao et al. [4]은 Flow Spectrum 대신 Masked AutoEncoder 기반의 자기지도학습 기법을 도입하여, 라벨 의존도를 줄여 높은 정확도를 달성하였다. 특히, 비라벨 데이터를 활용한 사전학습을 통해 실용성과 확장성이 뛰어났지만 MFR 형식에 대한 의존성과 일반화 가능성은 추가 검증이 필요하다. 그럼에도 YaTC는 트래픽 분류 정확도가 약 98%로 우수한 성능을 보이며, 자기지도학습 기반 트래픽 분류의 가능성을 보여준다.

ACKNOWLEDGMENT

이 논문은 2025년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임(RS-2024-00406796, 2025년 산업혁신인재성장 지원사업), 2025년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (RS-2023-00235509, ICT융합 공공 서비스·인프라의 암호화 사이버위협에 대한 네트워크 행위 기반 보안관제 기술 개발)

참고문헌

[1] Cui, Jun, et al., The Attention Based Autoencoder for Network Traffic Classification with Interpretable Feature Representation, Symmetry, 16, 5, 589, 2024.

[2] Yang et al, FlowSpectrum: a concrete characterization scheme of network traffic behavior for anomaly detection, World Wide Web, 25, 5, 2022, 2139 - 2161.

[3] Woo, Sanghyun, et al., CBAM: Convolutional Block Attention Module, Proceedings of the 15th European Conference on Computer Vision (ECCV), Munich, Germany, 2018, 3 - 19.

[4] Zhao, Ruijie, et al., Yet Another Traffic Classifier: A Masked Autoencoder Based Traffic Transformer with Multi Level Flow Representation, Proceedings of the 37th AAAI Conference on Artificial Intelligence (AAAI 23), Washington, DC, USA, 2023, 5420 - 5427.