# 암호화 트래픽 분류를 위한 MAE 기반 모델 어텐션 메커니즘 경량화 기법 분석

김태윤[1], 배기태[2], 김가영[3], 서주형, 김찬형[4], 이브라히모바-나일라, 윤종희[5]
영남대학교 컴퓨터공학과 학부과정[13], 석사과정[4], 교수[5]
영남대학교 로봇공학과 학부과정[2]
elma9810@yu.ac.kr, bgt010@naver.com, im_770@naver.com, blane7777@naver.com
qnfrha@yu.ac.kr, 22446177@ynu.kr, youn@yu.ac.kr

# An Analysis of Lightweight Attention Mechanisms in MAE-Based Models for Encrypted Traffic Classification

Tae-Yun Kim[1], Gi-Tae Bae[2], Ga-Young Kim[3], Ju-hyeong Seo,
Chan-hyung Kim[4], Ibrahimova Naila, Jong-Hee Youn[5]
Dept. of Computer Engineering, Yeung-Nam University[1345]
Dept. of Robotics Engineering, Yeung-Nam University[2]

요 약

인터넷 사용의 급증과 더불어 개인정보 보호 및 보안 강화의 중요성으로 인해 암호화 트래픽이 급증하였다. 이러한 암호화 트래픽의 증가로 악성 행위가 은폐되고 보안 솔루션의 가시성 또한 저하되는 문제점들이 야기되고 있다. 이러한 연유로 암호화 트래픽을 분류하는 연구들이 진행되고 있는데 최근 AI 기술의 발전으로 암호화 트래픽 분류 연구에 AI 기술 많이 연구되고 있다. 그 중 MAE(Masked Auto-Encoder)기반 모델이 좋은 성능으로 주목받고 있는데 MAE 기반 모델의 학습 연산은 상당한 비용과 시간이 필요한 문제점이 있다. 본 논문에서는 이러한 문제점을 해결하기 위한 방안으로 어텐션 메커니즘의 경량화 기법에 대해서 고찰하고자 한다.

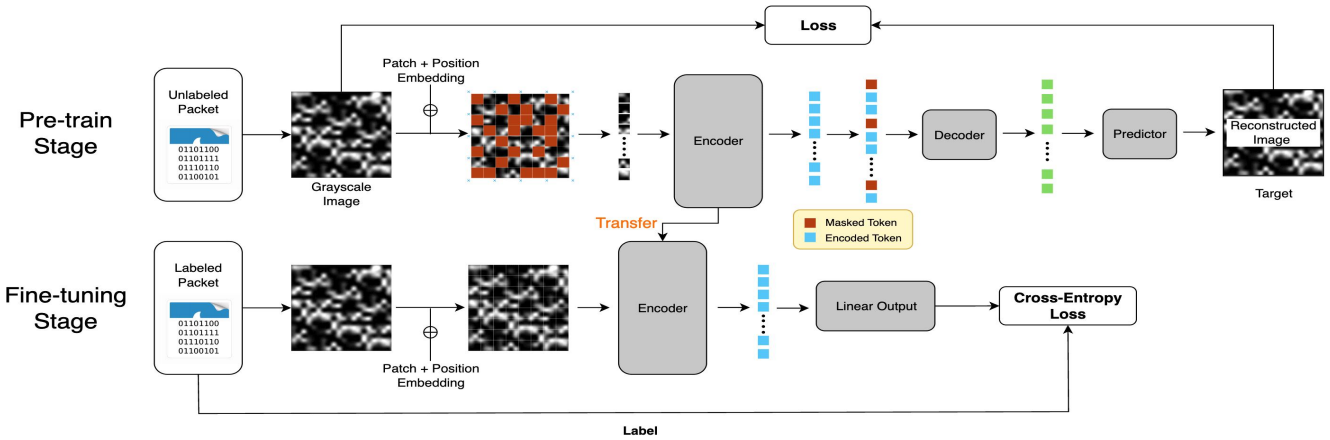
## 1. 서론

모바일 및 IoT 기기의 등장으로 인터넷 사용자의 폭증과 더불어 개인정보 보호와 보안 강화의 중요성이 높아짐에 따라 인터넷 트래픽의 대부분이 HTTPS, TLS, VPN 등과 같은 암호화 기술로 암호화되어 전송되고 있다. 이는 암호화 기술의 발전으로 인해 페이로드 정보를 접근할 수 없게 되면서, 이는 단순한 통계적 기법이나 규칙 기반 방법 등의 전통적인 트래픽 분류 방식에 큰 도전을 안겨주고 있다 [1]. 최근 딥러닝과 같은 인공지능(AI) 기술이 발전하면서, 암호화된 트래픽의 패턴 및 특성을 학습 가능한 모델로 트래픽을 추출하여 분류하는 연구들이 활발히 진행되고 있다 [2]. 그 중 레이블이 부여되지 않은 트래픽을 효과적으로 활용하기 위한 자기지도학습 기반의 접근법, 특히 Masked Auto-Encoder 기반 모델은 주목할 만한 성과를 보여주고 있다. 하지만 MAE 기반 모델은 학습 연산량이 높고, 모델의 구조가 복잡하다는 점과 이러한 연유로 실제 인프라에 적용하기 어려운 한계점을 가지고 있다.

본 논문의 구성은 다음과 같다. 2장에서는 MAE 기반 모델과 모델별 문제점을 소개하고, 3장에서는 문제점을 개선하기 위한 어텐션 메커니즘의 경량화 방안을 제시하며 4장에서는 결론을 제시한다.

## 2. 관련 연구

Xu et al은 MAE(Masked Auto-Encoder) 기반의 악성 트래픽 분류 모델인 MTC-MAE(Malware Traffic Classfication-Masked AutoEncoder)를 제안했다 [3]. 그림 1은 MAE 기반 분류 모델의 구조 예시이다. 해당 모델은 MAE 기반 사전학습을 통해 인코더가 대규모 비레이블 악성 트래픽 데이터를 학습하고, 파인튜닝에서 레이블 데이터를 통해 학습한다. 그러나 위 모델은 높은 연산 복잡도와 암호화 트래픽과 비암호화 트래픽이 혼합된 데이터 셋에서 분류 성능이 떨어지는 단점이 있다. Zhao et al은 Fine-Tuning에서 두 개의 인코더를 설계하여 각각 PL(Packet-Level) 수준과 FL(Flow-Level) 수준의 국소적인 어텐션을 적용한 YaTC 모델을 제안했다 [4]. YaTC는 설계한 어텐션 메커니즘을 위해 패킷




<그림 1> Masked Auto-Encoder 기반 모델의 아키텍처 예시

$M$개를 쌓아올린 독자적인 데이터 포맷인 $MFR$ 행렬을 사용하였다. 이를 통해, PL Attention은 연산복잡도를 $O(N^2)$에서 $O(N^2/M)$으로 낮추었고 FL Attention은 패치들을 Pooling 작업을 통해 $N$개에서 $\sqrt{N}$개로 감소시켜 어텐션의 복잡도를 $O(N^2)$에서 $O(N)$으로 낮추었다. YaTC는 뛰어난 분류 성능을 보여주지만 이러한 노력에도 타 모델 대비 높은 연산 복잡도를 지니고 있어 분석 효율을 높이기 위한 연구가 진행되고 있다.

## 3. 경량화 방안

### 3-1) 연산 효율 개선 어텐션 메커니즘 설계

YaTC는 토큰을 국소 윈도로 분할하고, Token Pooling 기법을 통해 토큰의 수를 감소시켜 연산 복잡도를 개선하였다. 그러나 $MFR$의 입력 크기는 40*40으로 타 모델에 비해 크다. 따라서, 입력 크기를 축소한 새로운 데이터 포맷에 경량화된 어텐션 메커니즘을 적용한다면 더 나은 성능 향상을 기대할 수 있다.

### 3-2) LoRA 기법 적용

LoRA(Low-Rank Adaptation)는 어텐션 연산의 핵심 가중치 갱신을 Low-Rank 행렬로 제한하여 연산량을 줄이는 기법이다. 해당 기법은 어텐션 구조 변경없이, 일부 가벼운 파라미터만 추가 학습하도록 한다. LoRA 기법을 적용한다면 모델의 성능 저하 없이 파인튜닝 연산 복잡도 감소를 기대할 수 있다.

## 4. 결론 및 향후 연구 방향

본 논문에서는 암호화 트래픽 연구 최근 동향에 대해 간략하게 설명하고, MAE 관련 모델의 특성과 한계점을 소개하고 경량화 방안에 대해서 제시하였다. MAE 기반 모델들은 뛰어난 분류 성능을 보여주지만 연산 복잡도가 높다는 문제점이 있다. 따라서, 이를 개선하는 연구들이 진행 중이며 실시간 이상 탐지(IDS) 장비 등 실제 인프라에 적용하기 위한 노력이 이어지고 있다. 어텐션 메커니즘의 경량화를 통해 연산 복잡도를 낮춘다면 실제 인프라에 적용함으로써 보안 측면 뿐만 아니라 네트워크 관리(QoS) 측면에서도 뛰어난 기여를 할 것으로 예상된다.

## Acknowledgements

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

## 참고문헌

[1] Mali et al. “Encrypted Network Traffic Classification Using Intelligent Techniques”, in Cureus Journals, vol.2, no.1, (2025)

[2] Yang et al. “FlowSpectrum: a concrete characterization scheme of network traffic behavior for anomaly detection”, in World Wide Web, vol.25, no.5, page.2139-2161, (2022)

[3] Xu et al. “Self-Supervised Learning Malware Traffic Classification Based on Masked Autoencoder”, in IEEE Internet of Things Journal, vol.11, no.10, page.17330-17340, (2024)

[4] Zhao et al. “Yet Another Traffic Classifier: A Masked Autoencoder Based Traffic Transformer with Multi-Level Flow Representation”, in Proceedings of the AAAI Conference on Artificial Intelligence, vol. 37, no. 4 , pp. 5420-5427, (2023)