양자화 기법을 활용한 FlowSpectrum 기반* 암호화된 트래픽 분류 성능 개선 연구

김찬형[1], 윤종희[2]
[1]영남대학교 컴퓨터공학과 석사과정
[2]영남대학교 컴퓨터공학과 교수
qhfrha@yu.ac.kr, youn@yu.ac.kr

Performance Improvement of Encrypted Traffic Classification Based on FlowSpectrum Using Quantization Techniques

Chan-Hyung Kim[1], Jongeee Youn[2]
[1]Dept. of Computer Science, Yeungnam University
[2]Dept. of Computer Science, Yeungnam University

요 약

본 연구에서는 FlowSpectrum을 활용하여 암호화된 트래픽 분류의 성능을 개선하기 위한 양자화 기법을 제안한다. 통신 기술의 발전으로 인해 암호화된 트래픽의 양이 증가하고 있으며, 이는 네트워크 관리 및 보안 모니터링에 어려움을 초래하고 있다. FlowSpectrum은 오토인코더를 통해 암호화된 트래픽에서 추출된 데이터를 1차원 표준 좌표계에 다양한 간격의 스펙트럼 선으로 표현하는 새로운 특징으로, 복호화 없이도 데이터 추출이 가능하다. 본 연구에서는 FlowSpectrum 기반 암호화된 트래픽 분류에서 양자화 수준에 따른 분류 성능의 변화를 분석하였으며, 실험 결과 3자리 양자화에서 가장 높은 성능을 보였다. 이는 양자화가 FlowSpectrum의 특성을 효과적으로 활용할 수 있는 방법임을 시사하며, 향후 다양한 데이터셋에 대한 적용 가능성을 탐색하고 양자화 기법의 최적화를 통해 성능 향상을 도모할 예정이다.

1. 서론

통신 기술의 발전으로 우리 일상 생활과 밀접한 다양한 서비스들이 인터넷을 통해 제공되고 있다. 이에 따라 주민등록번호나 계좌번호 같은 민감한 개인정보를 온라인상에서 주고받는 일이 흔해졌고, 이런 정보를 보호하기 위해 암호화 통신이 필수가 되었다. 이로인해 인터넷 트래픽의 대부분이 암호화되고 있으며, 이는 사용자의 개인정보 보호와 보안 강화를 위한 핵심적인 조치로 자리잡았다[1]. 그러나 암호화된 트래픽의 증가는 네트워크 관리 및 보안 모니터링에 어려움을 초래하고 있다. 특히 기존의 페이로드 시그니처 기반 보안 장비들의 경우 암호화된 트래픽의 내용을 확인할 수 없어 쉽게 우회가 가능한 문제점이 있다. 이러한 상황에서 암호화된 트래픽을 복호화하지 않고도 분석할 수 있는 기술의 필요성이 커지고 있다.

본 논문의 구성은 다음과 같다. 2장에서 기존의 FlowSpectrum에 대한 선행연구를 분석한다. 3장에서는 성능 개선을 위한 새로운 방안을 제시하고, 4장에서 제안 방식과 종래방식의 결과를 비교 및 분석한다. 그리고 5장에서 결론을 맺는다.

2. 관련 연구

L Yang [2]등은 이상 트래픽을 탐지하기 위한 새로운 모델인 SemiAE를 제시하였다. SemiAE는 오토인코더를 통해 압축된 트래픽으로부터 추출한 FlowSpectrum을 활용하여 트래픽을 분류하는 모델이다. [2]에서는 SemiAE를 통해 NSL-KDD 데이터셋을 정상 트래픽과 비정상 트래픽으로 분류하는 실험을 진행하였으며 0.9513의 재현율을 보였다. 해당 연구는 경우 처음으로 FlowSpectrum을 제안하였다는 의의가 있지만, 암호화되지 않은 트래픽을 사용하였다는 한계가 있다.

J Cui [3]등은 SemiAE와 2차원 컨볼루션 신경망(2D-CNN)을 조합하여 암호화된 트래픽을 분류하는

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

모델인 Semi-2DCAE를 제안하였다. 해당 모델은 [2]와 동일하게 FlowSpectrum을 활용하여 트래픽을 분류하지만, 2차원 컨볼루션 신경망을 통해 추출한 원본 네트워크 트래픽의 공간 구조적인 특징도 표현하였다. [3]에서는 ISCX-VPN2016 데이터셋을 활용하여 트래픽을 분류하는 실험을 진행하였으며 약 98%의 재현율을 보였다. 해당 실험은 CNN을 활용하여 공간 구조적인 특징을 반영하였다는 의의가 있지만, 일부 데이터셋에서는 기존의 SemiAE 보다 낮은 성능을 보여주었다는 한계가 있다.

3. 분류 방식 제안

본 논문에서는 FlowSpectrum을 활용하여 암호화된 트래픽을 분류하고, 기존 연구와의 비교를 통해 성능을 개선하기 위한 방식을 제안한다.

3.1. 양자화

양자화(Quantization)란 모델의 실행 성능과 효율성 향상을 목적으로 신경망의 가중치와 활성화 함수의 출력을 더 작은 비트로 표현하는 경량화 기법이다. 본 논문에서는 FlowSpectrum의 각 스펙트럼 선 위치가 해당 트래픽의 특징을 나타낸다는 점에 주목하여, 양자화를 통해 FlowSpectrum을 보다 직관적으로 표현하고자 한다.

3.2. FlowSpectrum

FlowSpectrum이란 오토인코더를 통해 암호화된 트래픽에서 추출된 데이터를 1차원 표준 좌표계에 다양한 간격의 스펙트럼 선으로 표현한 새로운 특징(Feature)이다. 해당 특징의 경우 복호화를 하지 않아도 데이터의 추출이 가능하며, 이를 활용하여 트래픽을 분류하기 위한 다양한 연구가 수행되고 있다.

3.3. 실험 설계

실험 과정은 다음과 같다. 먼저, 기존과 동일하게 실수로 표현된 FlowSpectrum을 추출한 후, 소수점 자리수를 점진적으로 줄여가며 성능을 비교한다. 이를 통해 양자화된 FlowSpectrum이 효과적으로 트래픽 분류를 가능하게 하는지 평가할 것이다. 또한, 양자화의 정도에 따른 분류 성능의 변화를 분석하여 최적의 양자화 비율을 도출할 예정이다.

4. 실험 및 결과

본 연구에서는 제안된 양자화 기법을 적용한 FlowSpectrum의 성능을 평가하기 위한 실험을 진행하였다.

실험 데이터셋은 [3]과 동일하게 ISCX-VPN2016을 사용하였으며, 모델은 Semi-2DCAE를 사용하였다.

<표 1> 양자화 수준별 실험 결과

양자화 수준	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
기존	84.48	91.1	84.48	80.3
1	78.92	73.2	78.92	74.26
2	94.23	95.08	94.23	94.13
3	98.85	98.9	98.85	98.85
4	97.73	97.74	97.73	97.73
5	84.22	84.66	84.22	82.77
6	88.35	90.4	88.35	87.44
7	81.55	79.48	81.55	76.42

<표 1>은 양자화 수준별 실험 결과를 나타낸 표이다. 해당 표에서 양자화 수준은 표현한 소수점 자리수를 나타내며, 3자리까지 표현한 경우의 결과가 가장 우수하게 나타났다.

5. 결론

본 연구에서는 FlowSpectrum을 활용한 암호화된 트래픽 분류의 성능을 개선하기 위해 양자화 기법을 제안하였다. 실험 결과, 양자화 수준에 따라 분류 성능이 크게 달라짐을 확인하였으며, 특히 3자리 수준에서 가장 우수한 성능을 나타냈다. 이는 양자화가 FlowSpectrum의 특성을 효과적으로 활용할 수 있는 방법임을 시사한다. 향후 연구에서는 다양한 데이터셋에 대한 적용 가능성을 탐색하고, 양자화 기법의 최적화를 통해 향상된 성능을 달성할 수 있는 방안을 모색할 것이다.

참고문헌

[1] 최양서, 유재학, 구기종, 문대성. (2023). 네트워크 이상행위 탐지를 위한 암호트래픽 분석기술 동향. [ETRI] 전자통신동향분석, 38(5), 71-80.

[2] Yang, L., Fu, S., Zhang, X. et al. FlowSpectrum: a concrete characterization scheme of network traffic behavior for anomaly detection. World Wide Web 25, 2139 - 2161 (2022).
[3] Cui J, Bai L, Li G, Lin Z, Zeng P. Semi-2DCAE: a semi-supervision 2D-CNN AutoEncoder model for feature representation and classification of encrypted traffic. PeerJ Comput Sci. 2023;9:e1635. Published 2023 Nov 9.