CNN 기반 트래픽 분류기의 세션 내 패킷 순서를 반영한 차트 형태 입력 방법론

장윤성, 김지민, 김주성, 백의준, 김명섭*

고려대학교

{ brave1094, illiard1209, jsung0514, pb1069, tmskim* }@korea.ac.kr

Chart-shape Input Method Reflecting Temporal Packet Sequence for CNN-Based Traffic Classification

Yoon-Seong Jang, Ji-Min Kim, Ju-Sung Kim, Ui-Jun Baek, Myung-Sup Kim*

Korea Univ.

요 약

최근 CNN 기반 네트워크 트래픽 분류기 연구에서는 세션별 초기 784바이트를 추출한 뒤, 이를 28×28 형태의 정적 이미지로 변환하여 입력하는 방식이 주로 사용되었다. 그러나 이러한 방식은 네트워크 트래픽의 구조적 특징에는 집중하지만, 시계열적 정보는 반영하지 못하는 한계가 존재한다. 본 연구에서는 세션 내 각 패킷의 바이트 시퀀스를 행(row) 방향으로 나열하고, 해당 패킷들을 시간 순서대로 열(column) 방향으로 쌓은 차트 형태의 입력 이미지를 생성하여, CNN이 시계열 흐름까지 학습할 수 있도록 하는 방식을 제안한다. 세 가지 실제 트래픽 데이터셋을 대상으로 실험한 결과, 기존 방식 대비 최대 7.3%의 정확도 향상을 달성하였다. 제안된 입력 구조는 CNN 기반 분류기의 표현력을 확장하여, 구조적 특징과 시계열적 정보를 동시에 반영할 수 있음을 보여준다.

Ⅰ. 서 론

네트워크 트래픽은 전송되는 데이터 패킷의 연속으로, 이를 정확히 분류하는 일은 보안 및 트래픽 관리에 필수적이다. 기존 포트 기반이나 Signature 기반 분류 방법론은 암호화 기술과 프로토콜 복잡성 증가로 한계를 드러냈으며, 이를 보완하고자 최근에는 딥러닝 기반 기법이 주로 연구되고 있다. 그 중 CNN 기반 방식은 고정 길이의 바이트 시퀀스를 이미지로 변환해 공간적 패턴을 학습하지만, 시계열 정보를 반영하지 못하고 필드 간 의미를 유지하지 못하는 한계가 존재한다.

이에 본 연구는 패킷 바이트 시퀀스를 행 방향으로, 패킷 순서를 열 방향으로 배열한 차트형 입력 방식을 제안한다. 이를 통해 시계열 처리 모델 없이도 CNN만으로도 구조적인 특징에 시계열적 특징을 추가로 학습할 수 있으며, 정확도와 연산 효율을 모두 향상시킬 수 있다.

Ⅱ. 관련 연구

딥러닝 기반 트래픽 분류기 연구는 주로 CNN을 활용해 이미지 형태로 네트워크 세션 데이터를 변환하고 이를 분류하는 접근에 집중되어 왔다.

Wang 등은 세션에서 784바이트를 추출해 28*28 이미지로 변환한 후 2D-CNN을 적용해 애플리케이션 분류를 수행하였다【1]. 이후 동일 저자는 바이트 시퀀스를 직접 입력으로 받는 1D-CNN을 제안하여, 수동적인 특징 설계 없이도 End-to-end 학습이 가능하도록 개선하였다【2].이후 제안된 HAST-IDS는 CNN을 통해 패킷 단위의 공간적 특징을 추출하고, 이를 LSTM을 통해 시간 순서대로 처리하는 구조로, 공간과 시간 정보를 모두 활용하는 시도를 보여주었다. 특히 HAST-2는 CNN과 LSTM을 결합해 높은 탐지 성능과 낮은 오탐률을 달성하였으며, 시계열 기반 모델의 효과를 강조하였다【3].

그러나 위의 기존 연구들은 다음과 같은 한계를 가진다. 첫 번째로, 2D-CNN이나 1D-CNN 기반 모델은 세션 내 패킷의 시간 순서를 고려하지 않아 흐름의 시계열적 구조를 반영하지 못한다. 두 번째로는, 바이트 단위로 이미지를 생성하는 과정에서 멀티바이트 필드가 임의로 분리되며, 필드 간 의미가 손실되는 문제가 발생한다.

Ⅲ. 본 론

네트워크 트래픽은 헤더와 페이로드, 필드로 이루어지는 구조적(공간적)인 특징과 이어지는 각 패킷의 인과관계가 존재하는 시계열적 패턴을 포함하고 있으며, 이는 트래픽을 분류하는 데에 중요한 정보를 제공한다. 그러나 기존 CNN 기반 트래픽 분류 모델은 이러한 시계열 정보를 고려하지 않고, 바이트 값을 정적 배열로 변환해 이미지 형태로 처리하면서 구조적인 특징만을 사용하여 분류하였다. 기존에 주로 사용되었던 세션-이미지 변환 방식은 m개의 패킷에서 n바이트를 추출한 뒤, 이를 가로 방향으로 이어 붙이고 28바이트씩 잘라 세로 방향으로 배열해 28*28 이미지를 구성하는 방식이지만, 이 과정에서 패킷 간 시간 흐름 정보는 손실된다.

본 연구에서는 이러한 한계를 보완하기 위해 입력 이미지를 차트 구조로 재구성하는 방식을 제안한다. 이 방식은 세션 내 각 패킷의 바이트 시퀀스를 행 방향으로 나열하고, 해당 패킷들을 시간 순서대로 열 방향으로 배치하여, CNN이 시계열적 변화와 공간 구조를 동시에 학습할 수 있도록 한다. LSTM 없이도 시간에 따른 패턴을 CNN 내에서 직접 학습할 수 있게 하여 정확도와 처리 효율을 개선할 수 있다.

입력 데이터는 기존 방식과 동일하게 전처리하였으며, 실험에서는 L3(IP), L4(TCP/UDP)의 포함 여부에 따라 4가지 조건을 설정하였다. 이더넷 헤더는 모두 제거하였고, 학습/테스트는 8:2 비율로 분할하였다. 기존 방식은 28*28 입력을 고정으로 사용하였지만, 제안된 방식은 동일한 총 바이트 수 784를 유지하면서 4*196, 7*112, 8*98, 14*56, 형태의 다양한 약수쌍을 실험에 사용하였다. 7*112 구조가 전반적으로 높은 정확도를 나

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(00230661, 하이브리드 양자키분배 방법 및 망 관리 기술 표준개발) 및 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(00235509, ICT융합 공공 서비스• 인프라의 암호화 사이버위협에 대한 네트워크 행위기반 보안관제 기술 개발)을 받아 수행된 연구임.

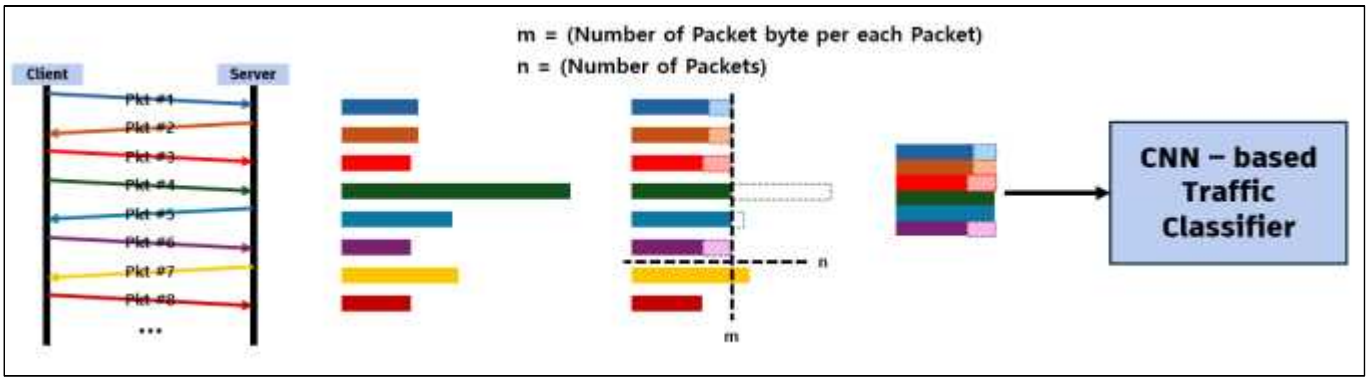

그림 1. 제안된 차트 형태 입력 방식의 구조도

타냈으며, 일자 형태(1*784, 2*392)와 과도한 패딩이 필요한 16×49, 28*28 구조는 제외되었다. 본 연구는 입력 구조의 단순한 변화만으로도 CNN이 시계열 패턴을 효과적으로 학습할 수 있음을 실험적으로 확인하였다.

Ⅳ. 실험 평가

본 연구는 제안된 차트 기반 입력 방식의 효과를 검증하기 위해 ISCX VPN2016, PRIVATE#1, PRIVATE#2의 세 가지 데이터셋을 사용하여 실험 평가를 수행하였다. 이 중 PRIVATE#1과 PRIVATE#2는 동일한 50개의 응용프로그램을 대상으로 서로 다른 환경에서 수집된 데이터셋이다.

ISCX VPN2016 데이터셋에서는 4*196 형태의 입력 구조가 가장 우수한 성능을 기록하였으며, 기존 2D-CNN 기반 방식 대비 약 3.1%의 정확도 향상을 보였다. PRIVATE#1 데이터셋에서는 14*56 입력 구조에서 가장 높은 정확도가 나타났으며, 기존 방식에 비해 최대 7.3%p 향상된 성능을 기록하였다. 이는 복잡한 애플리케이션 분류 환경에서도 제안된 방식의 시계열 정보 반영이 효과적임을 보여준다. PRIVATE#2 데이터셋에서는 7*112 구조가 가장 뛰어난 결과를 보였으며, 기존 대비 약 3.4%의 정확도 개선이 확인되었다.

이와 같은 결과는 세션 내 패킷 순서를 고려한 차트형 입력 방식이 기존 CNN 모델의 한계를 극복하고, 시계열 정보와 구조적 의미를 동시에 학습할 수 있게 함으로써 네트워크 트래픽 분류 성능을 효과적으로 향상시킨다는 것을 보여준다.

표 1. 실험 결과 정리(Accuracy)

Dataset	ACC	L3 O	L4 O	L3 O	L4 X	L3 X	L4 O	L3 X	L4 X
VPN 2016	2D-CNN	0.7089	0.7079	0.6945	0.7029				
VPN 2016	4*196	0.7259	0.7319	0.7244	0.7339				
VPN 2016	7*112	0.7104	0.7164	0.7134	0.7204				
VPN 2016	8*98	0.7204	0.7099	0.7094	0.7204				
VPN 2016	14*56	0.7079	0.6935	0.6995	0.7069				
PRIVATE #1	origin	0.7222	0.7151	0.7119	0.7231				
PRIVATE #1	4*196	0.7587	0.7528	0.7658	0.7624				
PRIVATE #1	7*112	0.7818	0.7761	0.774	0.7786				
PRIVATE #1	8*98	0.7761	0.7788	0.7832	0.7742				
PRIVATE #1	14*56	0.7945	0.7889	0.7918	0.7912				
PRIVATE #2	origin	0.7572	0.7707	0.7537	0.7665				
PRIVATE #2	4*196	0.7957	0.7909	0.799	0.7987				
PRIVATE #2	7*112	0.8017	0.7976	0.7999	0.8032				
PRIVATE #2	8*98	0.8002	0.8038	0.8032	0.793				
PRIVATE #2	14*56	0.7984	0.7984	0.7987	0.7984				

Ⅳ. 결 론

본 논문은 네트워크 트래픽의 시계열성과 구조적 특성을 동시에 반영하기 위해, 패킷 순서를 고려한 차트 형태의 입력 방식을 CNN 기반 분류기에 적용하였다. 기존 CNN 모델은 28*28 형태의 이미지를 생성하는 전처리 과정에 의해 시간 흐름에 따른 바이트 변화와 같은 중요한 특성을 학습하기 어려웠으며, 각 필드 고유의 의미가 손실되는 한계가 존재하였다. 제안된 방식은 세션 내 각 패킷의 바이트 시퀀스를 행방향으로 나열하고, 해당 패킷들을 시간 순서대로 열방향으로 구성하여 CNN만으로도 시계열 정보를 학습할 수 있도록 설계되었다. 이를 통해, 시간에 따라 각 패킷의 변화하는 패턴을 학습하도록 하였으며, 각 필드로부터 생성된 칸이 인접하여 그 고유의 의미의 손실을 최소화 하였다. 실험 결과, ISCX VPN 2016에서는 4*196 구조에서 기존 2D-CNN 대비 3.1% 정확도 향상이 있었고, PRIVATE#1과 PRIVATE#2에서는 각각 14*56과 7*112 구조에서 최대 7.3%, 3.4%의 성능 향상이 나타났다. 이는 단순한 입력 구조 조정만으로도 CNN의 표현력을 확장할 수 있음을 보여준다.

연구의 주요 기여는 CNN 프레임워크 내에서 시계열 정보를 반영할 수 있는 새로운 입력 구성 방식을 제안한 점이며, 트래픽과 같이 복합적인 데이터에 대한 CNN의 적용 가능성을 넓혔다. 다만 데이터셋별로 최적 입력 구조가 달랐던 원인과, 바이트 단위 처리로 인한 필드 의미 손실은 향후 보완이 필요하다. 또한, 악성 트래픽 분류 연구에서는 각 세션은 매우 짧은 시간 유지되므로, 분류에 사용될 단서가 적으므로, 제안된 방법론의 효과가 미비할 것으로 예상된다. 따라서 향후에는 필드 단위 마스킹 및 프로토콜별 구조 최적화를 통해, 입력 정보의 중요도를 정량적으로 분석하고 악성 트래픽 분류 분야에서 다중 세션 단위의 입력을 활용한 패턴의 분석으로 분류하는 연구를 제안한다.

참 고 문 헌

[1] Wei Wang, Ming Zhu, Xuewen Zeng, Xiaozhou Ye, Yiqiang Sheng, Malware traffic classification using convolutional neural network for representation learning, in: 2017 International Conference on Information Networking (ICOIN), IEEE, 2017, pp. 712 - 717.

[2] Wei Wang, Ming Zhu, Jun Wang, Xuewen Zeng, Zhihua Yang, End-to-end encrypted traffic classification with one-dimensional convolution neural networks, in: 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), IEEE, 2017, pp. 43 - 48.

[3] Wei Wang, Yiqiang Sheng, Jinlin Wang, Xuewen Zeng, Xiaozhou Ye, Yongzhong Huang, Ming Zhu, HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection, in: IEEE Access, vol. 6, 2018, pp. 1792 - 1806.