논문 25-28-02-04
KNOM Review '25-02 Vol.28 No.02
https://doi.org/10.22670/knom.2025.28.2.33

세션 및 패킷 번들 단위에서의 WeChat 행위 분석

김 지 민◆, 김 란 아*, 장 윤 성**, 백 의 준***, 김 명 섭°

WeChat Behavior Analysis with Session and Packet Bundle Level

Ji-min Kim◆, Ran-A Kim*, Yoon-Seong Jang**, Ui-Jun Baek***, Myung-Sup Kim°

요 약

현대 네트워크 환경에서는 암호화로 인해 페이로드 기반 분석이 어려워지면서, 세션과 패킷의 통계적 특성을 활용한 행위 기반 트래픽 분석의 중요성이 커지고 있다. 본 연구는 WeChat 트래픽을 대상으로, 세션 구조와 시간적 패턴을 통합 학습하는 이중 Convolutional Neural Network(CNN) 기반 행위 분석 프레임워크를 제안하였다. 특히 동일 세션 내의 행위 분석이 불가능하다는 세션 단위 분석의 한계를 보완하기 위해 '패킷 번들(Packet Bundle)' 개념을 새롭게 도입하여 세션 내부의 시간 구간별 패턴 변화를 정량적으로 분석하고, Chat과 File Transfer와 같은 동일 세션 내 발생 행위를 효과적으로 구분하였다. 제안된 모델은 세션 단위의 2D CNN과 패킷 번들 단위의 1D CNN을 결합하여 Voice, Video, Chat/File Transfer, Others 세션을 높은 정확도로 분류하였으며, 1D CNN은 평균 97%의 정확도를 기록하였다. 또한 WhatsApp, KakaoTalk 데이터셋에서도 유사한 성능을 보여 방법의 범용성과 실용성을 입증하였다. 본 연구는 세션 및 패킷 번들 기반의 시공간적 특징 학습을 통해 암호화된 환경에서도 세밀한 행위 인식이 가능한 효율적 분석 프레임워크를 제시한다.

Key Words : Network Traffic Classification, WeChat Behavior Analysis, Packet Bundle

ABSTRACT

In modern network environments, encryption has made payload-based analysis increasingly difficult, highlighting the importance of behavioral traffic analysis that leverages the statistical characteristics of sessions and packets. This study proposes a dual CNN-based behavioral analysis framework that jointly learns the structural and temporal patterns of WeChat traffic. To address the limitations of session-level analysis, a new concept called the "Packet Bundle" is introduced to quantitatively analyze temporal variations within sessions and effectively distinguish similar behaviors such as Chat and File Transfer. The proposed model combines a session-level 2D CNN with a packet-bundle-level 1D CNN to classify Voice, Video, Chat/File Transfer, and Others sessions with high accuracy, achieving an average classification accuracy of 97% for the 1D CNN. Furthermore, comparable results obtained on a WhatsApp, KakaoTalk dataset demonstrate the generalizability and practicality of the proposed approach. This study presents an efficient analysis framework capable of fine-grained behavior recognition in encrypted environments through packet-bundle-based spatio-temporal feature learning.

※ 이 논문은 과기정통부·정보통신기획평가원의 정보통신방송표준개발지원(R&D,정보화)사업으로 수행한 결과(No. RS-2025-02219319, 양자컴퓨터 공격에도 안전한 양자암호기반 제로트러스트 보안 네트워크/서비스 및 제어/관리 기술 표준개발), 2025년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(RS-2025-16067207)

◆ First Author : Korea University Department of Computer Convergence Software, illiard1209@korea.ac.kr
° Corresponding Author : Korea University Department of Computer Convergence Software, tmskim@korea.ac.kr
* Korea University Department of Mobility Science and Engineering, zufrieden7@korea.ac.kr
** Korea University Department of Computer Convergence Software, brave1094@korea.ac.kr
*** Korea Institute of Science and Technology Information (KISTI), pb1069@kisti.re.kr

논문번호 : KNOM2025-02-007, Received November 10, 2025; Revised November 24, 2025; Accepted December 11, 2025

Ⅰ. 서 론

네트워크 기술이 발달함에 따라 이를 체계적으로 관리하고 모니터링하는 기술에 필요성이 늘어나고 있다. 그 중 트래픽 분류는 이상 트래픽을 탐지하거나, 사용자의 행위를 분석하는 등 여러 확장성을 가지고 있어 네트워크 관리 기술에서 중요한 역할을 하고 있다.

네트워크 기술 발전에 따라 트래픽 분류 방법 또한 발전하였는데, 규칙 기반(Rule-based) 접근 방식인 포트 기반[1], DPI(Deep Packet Inspection) 기반[2]과 머신러닝 접근 방식인 통계 기반[3], 그리고 행위 기반[4] 방법이다. 그러나 동적 포트의 등장과, 암호화된 페이로드로 인하여 규칙 기반의 분류 기법들은 사용하는 데에 한계가 있으며, 머신러닝 기법의 경우 특징을 직접 추출하므로 적절한 특징을 설계해야 한다는 점과 개발자의 역량에 의해 분류 정확도가 변화한다는 한계점이 존재한다.

이를 해결하기 위하여 여러 가지 딥러닝 모델들을 트래픽 분야에 접목하여 트래픽 분류를 하는 연구들이 등장하고 있다. 세션을 이미지로 입력하여 네트워크 분류를 하는 CNN 모델 [5]과, 시계열 데이터적 관점에서 처리하는 RNN/LSTM [6]모델 그리고 트래픽을 자연어의 관점에서 바라보는 Transformer 모델 [7]까지 등장하였다. 그러나 이러한 DL 모델들도 기존의 트래픽적 특징을 보존하여 입력으로 사용하는 방법을 채택하고 있지 않기에 네트워크 트래픽 분류 방법론에 발전 가능성을 두고 있다.

네트워크 트래픽 분석 분야는 단순한 패킷 분류를 넘어 여러 세부 업무로 확장되고 있다. 대표적인 예로 응용 서비스 식별, 이상 탐지, 사용자 행위 분석 등이 있다.

이 중 사용자 행위 분석은 특정 응용을 사용한 사용자의 트래픽을 통해 사용자의 행위를 분류하고 분석하는 것이다. 단순히 트래픽의 형태나 클래스에 의존하지 않고, 세션 간의 시간적 상관관계, 패킷 전송의 주기성, 흐름 간 상호작용 등 행위적 특성과 통계적 특징을 추출함으로써 사용자의 목적, 사용 행태, 혹은 비정상적 패턴을 식별할 수 있다.

이러한 행위 분석은 암호화된 환경에서도 페이로드 정보 없이 트래픽의 의미적 변화를 파악할 수 있으며, 단순 분류를 넘어 지능형 네트워크 관리, 보안 위협 탐지 등 다양한 응용 분야로 확장 가능하다는 점에서 그 중요성이 커지고 있다.

본 연구에서는 행위 기반 트래픽 분석의 대상으로 WeChat을 선정하였다. WeChat은 Tencent가 개발한 통합형 모바일 플랫폼으로 채팅, 음성 및 영상 통화, 파일 전송 등 다양한 기능을 하나의 애플리케이션 내에서 제공한다.

본 연구에서는 WeChat 트래픽을 대상으로 사용자의 행위적 특성을 분석하기 위해 세션을 총 네 가지 유형으로 구분하였다.

WeChat 어플리케이션의 경우 mmTLS라는 독자적인 암호화 프로토콜을 사용한다. mmTLS는 전송 구간의 기밀성과 무결성을 보장하기 위해 TLS 기반 구조를 확장한 형태로, 일반 HTTPS 트래픽보다 더 복잡한 세션 구조와 비표준 핸드셰이크 과정을 포함한다. 이러한 특성으로 인해 페이로드 분석이나 세션 복호화가 사실상 불가능하지만, 본 연구에서는 암호화 프로토콜의 내부 동작을 해석하지 않고도 세션 구조와 패킷 통계 정보를 기반으로 행위 식별이 가능함을 제시한다.

WeChat의 주요 기능 중 Chat과 File Transfer는 채팅방 내에서 이루어지는 행위이며, 동일한 세션 내에서 패킷이 발생한다는 특징이 있어 ChatRoom이라는 하나의 클래스로 통합하였으며, Voice, Video, Others 세션은 명확히 구분할 수 있는 행위 패턴을 보여 독립적인 클래스로 정의하였다. 이러한 네 가지 세션 유형을 대상으로 2D CNN 기반 분류 모델을 적용하여 행위적 특징을 학습하고 분류한다. ChatRoom에 존재하는 Chat/File Transfer 클래스는 하나의 세션에 묶여있는 특징이 있어 이를 보완하기 위해 시간 기반의 패킷 번들(Packet Bundle)의 통계적 특징을 추출하여 사용하는 1D CNN로 분류 방법론을 제시한다.

Ⅱ. 관련 연구

기존 연구에서는 암호화된 트래픽 환경에서 사용자 행위를 구분하기 위한 다양한 시도가 이루어졌다.

[8]은 Sliding Window 기반의 세션 세분화 기법을 제안하였다. 이 방법은 슬라이딩 윈도우의 좌측과 우측 패킷 분포를 비교하여 Kullback-Leibler (KL) Divergence를 계산하고, 이를 통해 트래픽 내 분포적 변화 지점을 탐지함으로써 행위 단위로 데이터를 구분하고자 하였다. 이러한 접근은 원시 데이터에서 직접 행위 구간을 탐색한다는 점에서, 트래픽 내 분포적 차이를 학습하는 새로운 시도를 제시하였다.

[9]는 Netmate 툴을 활용하여 세션 및 플로우 단위에서 44가지의 통계적 특징을 추출한 뒤, 이를 Naïve Bayes, Bayes Net, MLP 등 여섯 가지 머신러닝 분류기에 적용하여 WeChat 트래픽을 분류하였다. 이 연구는 WeChat 트래픽을 대상으로 한 통계적 특징 기반 분류 접근의 타당성과 적용 가능성을 제시하였으며, 추후 비페이로드 환경에서도 활용 가능한 특징 설계의 기초를 제공하였다.

기존 연구들은 암호화된 트래픽 환경에서 세션 단위로 행위를 구분하기 위한 다양한 시도를 제시하였으나, 여전히 몇 가지 한계가 존재한다.

첫째, WeChat과 같은 통합형 플랫폼에서는 Chat과 File Transfer가 동일한 세션 내에서 혼재되어 발생함에도 불구하고, 두 행위를 구분할 수 있는 명확한 기준이 제시되어 있지 않다. 두 행위가 하나의 세션에 묶여있어 세션이 분류 기준으로 되어있는 방법론이 적용되지 않는다는 한계점이 존재한다.

둘째, 기존 연구 대부분은 패킷의 분포나 시계열적 특성에 기반한 접근으로, 각 행위별 통계적 특징을 충분히 고려하지 못하였다.

이러한 한계를 극복하기 위해서는, WeChat에서 발생하는 행위 단위의 트래픽을 세션 및 패킷 번들 수준에서 정밀하게 분석하고, 이를 효율적으로 분류할 수 있는 새로운 방법론이 요구된다.

따라서 본 연구에서는 WeChat의 중요 행위인 Chat, File Transfer, Voice, Video를 포함한 실제 시나리오 데이터를 수집하여, 각 행위별 트래픽의 통계적·시간적 정보를 프레임워크에서 활용하였다. 이를 바탕으로 행위 구분이 어려운 세션 구조를 보완하고, 암호화된 환경에서도 세션의 행위적 패턴을 정량적으로 인식할 수 있는 새로운 분석 프레임워크를 제안한다.

Ⅲ. 본론

3.1. 데이터셋 수집 및 전처리

표 1. WeChat 데이터셋의 클래스별 세션 및 패킷 수
Table 1. Number of Sessions and Packets per Class in the WeChat Dataset

Class	Session	Packet
ChatRoom	25	7356
Voice	598	43767
Video	516	73719
Other	2628	25902

WeChat 트래픽 데이터는 실제 환경에서 다양한 행위 시나리오를 수행하여 수집하였다. 각 행위는 독립된 시간 구간으로 구성되며, 트래픽 수집 도구를 통해 세션 단위의 pcap 데이터로 저장하였다.

그림 1은 WeChat 트래픽 데이터 수집 과정을 나타낸 것이다. 실험은 실제 사용자 단말 환경에서 총 150초 동안 수행되었으며, WeChat 내의 다양한 기능(Voice, Video, Chat, File Transfer, Others)을 순차적으로 실행하여 트래픽을 캡처하였다. 캡처된 원본 트래픽은 pcap 형식으로 저장되었으며, 이후 세션 단위로 분리하여 분석에 활용하였다.

먼저, 원본 pcap 파일을 5-tuple을 기준으로 세션 단위로 구분하였다. 이후 각 세션은 실제 수행된 기능에 따라 Voice, Video, ChatRoom, Others로 라벨링되었다. 이렇게 라벨링된 세션들은 이후 통합 과정을 거쳐, 모델 입력 형식에 맞게 전처리되었다.

세션 단위 입력을 사용하는 2D CNN 모델의 경우, 각 세션에서 이더넷 헤더를 제거하거나 페이로드 부분만 추출하였다. 그 후 패킷 크기 및 전송 순서를 기반으로 2차원 행렬 형태로 변환하여, 세션의 시계열적 분포 특성이 보존되도록 구성하였다.

1D CNN 모델은 세션 내부의 세부 행위를 구

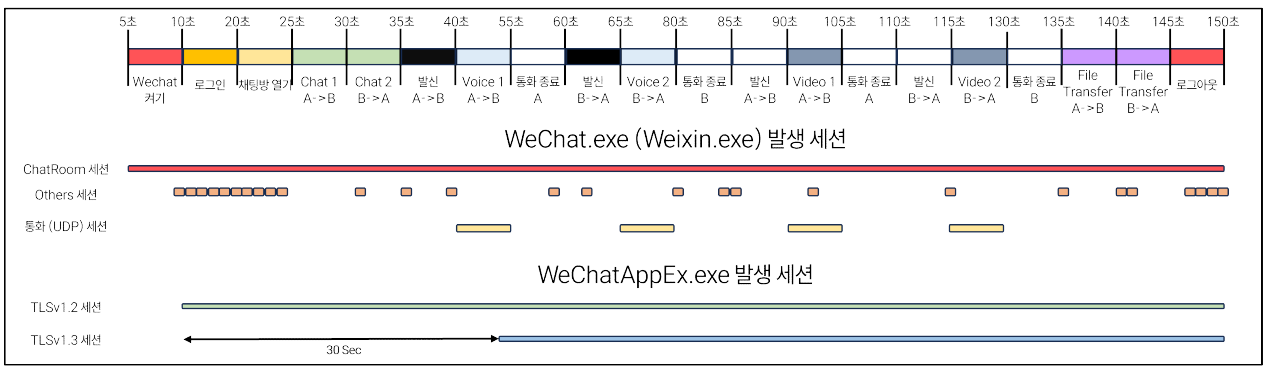

그림 1. WeChat 애플리케이션 사용 시 기능 별 세션 발생 패턴
Fig. 1. Session occurrence pattern by function during WeChat usage

분하기 위해 Chatroom 환경에서 수집된 트래픽을 기준으로 하였다. 수집된 시나리오 내 시간 정보를 활용하여, 채팅 메시지 송수신 구간과 파일 전송 구간을 분리하였으며, 이를 각각 독립된 패킷 번들 단위 입력 데이터로 구성하였다. 이러한 방식으로 세션 간 구조적 유사성이 높은 Chat과 File Transfer 구간을 시간적 특성에 따라 세분화함으로써, 모델이 세션 내 행위 단위 패턴을 학습할 수 있도록 전처리를 수행하였다.

3.2. WeChat 발생 트래픽 유형

WeChat 사용 시 WeChat.exe (現Weixin.exe)와 WeChatAppEx.exe 두 가지 프로세스가 발생하는 것을 확인하였다.

WeChat.exe의 경우 크게 네 가지 유형의 세션으로 구분할 수 있었는데, ChatRoom, Voice, Video, mmtls 세션으로 구분하였다. 해당 세션들에 대한 설명은 다음와 같다.

- ChatRoom : 채팅방 내에서 발생하는 패킷들을 포함하는 세션이다. 동일한 세션 내에서 Chat과 File Transfer 패킷이 발생한다.
- Voice : 음성 통화 시 발생하는 세션으로, 일정한 전송 주기와 양방향 데이터 흐름이 특징이다.
- Video : 영상 통화 과정에서 발생하는 세션으로, Voice보다 높은 전송률과 불균형한 데이터 흐름을 보인다.
- Others : 인증, 상태 동기화 등 제어 목적의 세션으로, 비교적 짧은 지속 시간과 작은 데이터 단위를 가진다.

3.3. 행위 분석 프레임워크

3.3.1. 세션 단위 2D CNN

세션 단위의 트래픽 특성을 직접 학습하기 위해, 제안된 세션 단위 분류 모델은 각 세션의 패킷 데이터를 2차원 이미지 형태로 변환하여 2차원 합성곱 신경망(2D CNN) 기반으로 학습하도록 설계되었다. 그림 2의 좌측은 세션 단위 분류 과정과 모델의 전체 구조를 보여준다.

먼저, 수집된 pcap 데이터는 세션별로 분할된 후 공통적으로 L2 헤더를 제거하였다. 이후 연구 목적에 따라 L3 및 L4 헤더 제거 여부를 선택적으로 적용하고, 세션 내 첫 번째 패킷부터 최대 784바이트를 추출하였다. 추출된 바이트열은 28×28 크기의 2차원 행렬로 재구성하여 세션 이미지를 생성하였으며, 세션 길이가 부족한 경우에는 Zero-padding을 적용해 입력 크기를 고정하였다. 이 과정을 통해 트래픽의 바이트 시퀀스가 시각적 패턴 형태로 변환되어, CNN이 세션 구조적 특징을 자동으로 학습할 수 있도록 하였다.

제안된 모델은 두 개의 합성곱 계층과 두 개의 완전연결층으로 구성된 기본형 2D CNN 구조를 따른다. 첫 번째 합성곱 계층은 5×5 크기의 필터 32개를 사용하여 입력 이미지(1×28×28)로부터 지역적 바이트 분포를 추출하고, ReLU 활성화 함수를 통해 비선형성을 부여한다. 이후 2×2 크기의 Max Pooling 연산을 수행하여 특징 맵의 크기를

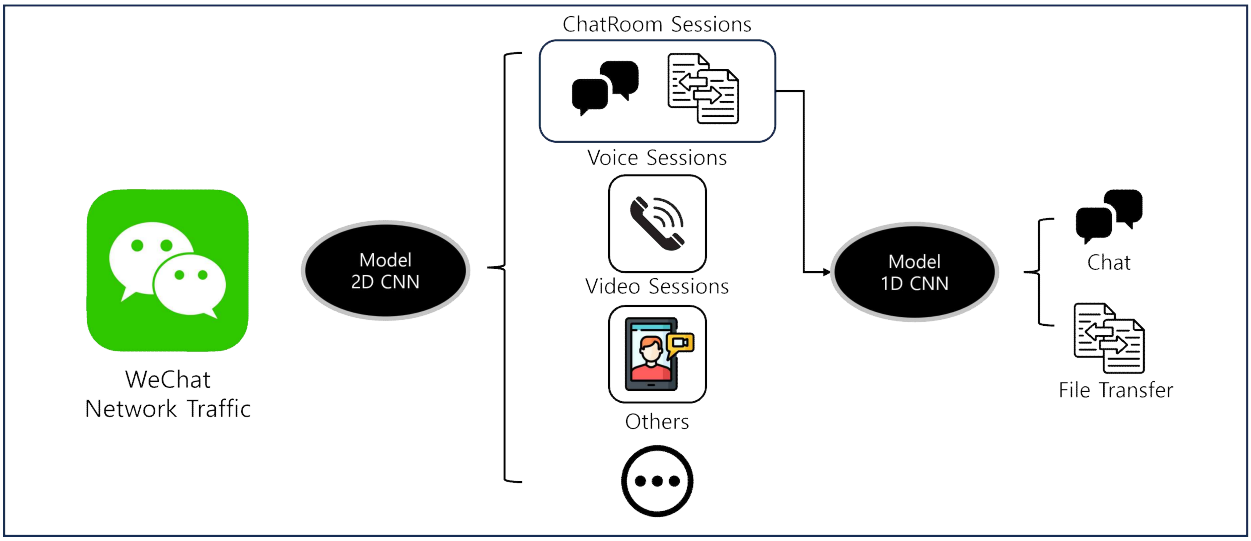

그림 2. 이중 CNN 기반 행위 분석 프레임워크

Fig 2. Dual CNN-based Behavioral Analysis Framework

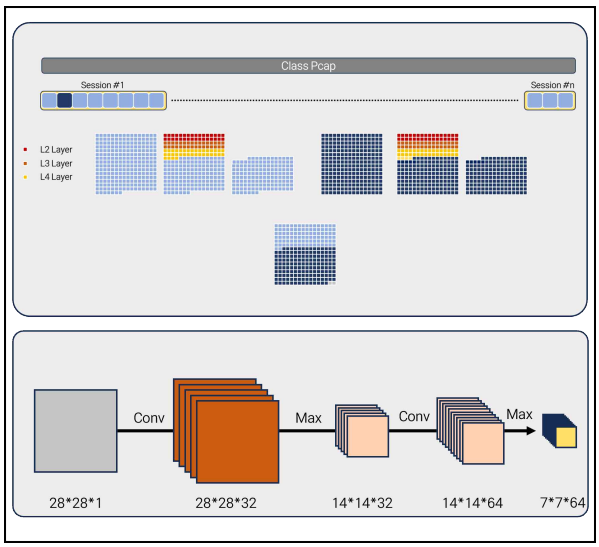

그림 3. 세션 단위 2D CNN 구조도
Fig 3. Session Level 2D CNN Architecture

(32×14×14)로 축소한다. 두 번째 합성곱 계층은 5×5 크기의 필터 64개를 사용하여 더 추상화된 세션 구조적 특징을 학습하며, 동일한 Max Pooling 연산을 통해 (64×7×7)의 출력 특징 맵을 얻는다.

이후 Flatten 과정을 통해 특징 맵을 3,136차원(=64×7×7)의 벡터로 변환하고, 첫 번째 완전연결층(1,024 뉴런)에서 ReLU 활성화와 0.5의 Dropout을 적용한다. 마지막 완전연결층은 네 개의 뉴런으로 구성되어 Voice, Video, Chat/File Transfer, Others 클래스에 대한 확률을 출력한다. 학습 과정에서는 교차 엔트로피(Cross Entropy) 손실 함수를 사용하고, 학습률 0.001를 적용하여 학습하였다.

제안된 2D CNN 모델은 세션 단위에서 발생하는 평균 패킷 크기, Burst 간격, 전송 방향 비율과 같은 통계적 특성을 별도의 수동 특징 설계 없이 자동으로 학습한다. 또한 세션 이미지를 통해 트래픽의 내부 구조(패킷 분포, 밀도, 주기성 등)를 시각적 패턴으로 인식함으로써, Voice·Video·Others와 같이 구조적 차이가 명확한 트래픽 유형을 분류할 수 있다.

3.3.2. 패킷 번들 단위 1D CNN

본 연구에서는 세션 내부의 시간적 행위 단위를 세밀하게 구분하기 위해 패킷 번들(Packet Bundle) 개념을 도입하였다. 이는 10ms 시간 간격 내에 발생한 연속적인 패킷 묶음을 의미하며, 세션을 시간 기반으로 세분화하여 세션 내 행위 변화(예: 채팅, 파일 전송 등)를 구분하기 위한 분석 단위로 활용된다. 세션 단위 분석만으로는 동일한 세션 내에 존재

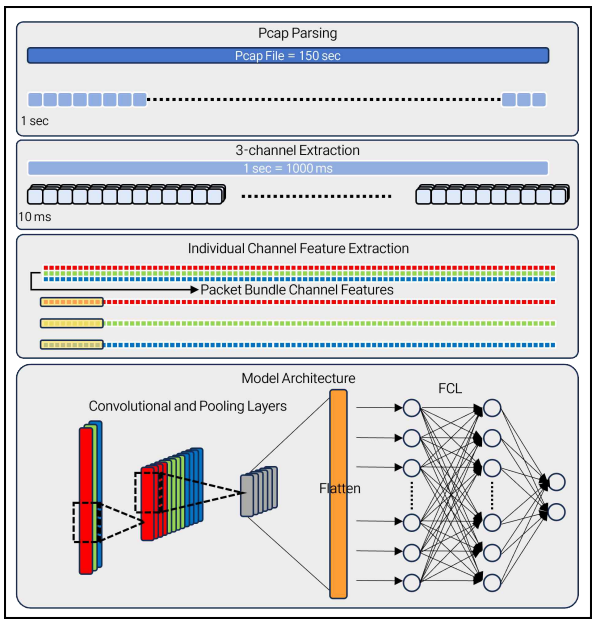

그림 4. 패킷 번들 단위 1D CNN 구조도
Fig 4. Packet Bundle Level 1D CNN Architecture

하는 Chat과 File Transfer 행위의 세밀한 구분이 어려우므로, 세션을 일정 시간 구간으로 분할하고 각 구간을 패킷 번들로 정의하여 1D CNN 기반 시계열 분석을 수행하였다.

수집된 pcap 데이터는 사전에 라벨링된 Chat과 File Transfer 트래픽을 기준으로 1초 단위로 분할하였으며, 각 구간 내에서 10ms 단위의 세부 구간별 (1) 누적 바이트 크기, (2) 패킷 개수, (3) 평균 패킷 간 간격(IAT)을 추출하여 각각 하나의 채널로 구성하였다. 따라서 최종 입력은 (3,L) 형태의 시계열 텐서이며, 이는 세 가지 상이한 통계적 속성을 동시에 표현한다.

제안된 1D CNN은 세 채널의 특성을 개별적으로 학습하기 위해 3개의 독립적인 합성곱 경로(branch)를 둔다. 각 branch는 입력 채널 1개를 받아 Conv1D(1→16, kernel_size=3, stride=1, padding=1), ReLU, MaxPool1D(kernel_size=2) 연산을 수행한다. padding을 1로 설정하여 시간축 길이를 유지한 채, 인접한 약 30ms 범위 내의 지역 패턴을 학습하며, Pooling을 통해 중요 특징만을 추출한다.

이후 세 branch의 출력(3×16=48채널)을 채널 축으로 연결(concatenate)하여 통합 시계열 표현을 구성한다. 이후 단계에서는 Conv1D(48→96, kernel_size=3, stride=1, padding=1) 과 ReLU, MaxPool1D(kernel_size=2) 를 적용하여 채널 간 상관관계와 상위 시계열 패턴을 함께 학습한다.

이러한 두 단계의 합성곱 및 풀링 과정을 거친 출력

텐서는 Flatten을 통해 1차 벡터로 변환되고, Fully Connected Layer를 통해 Chat과 File Transfer 클래스로 분류된다. 모델은 교차 엔트로피 손실 함수를 사용하고, 학습률 0.001를 적용하여 학습하였다.

이 구조는 각 3개의 채널에서 패킷의 개수가 급증하거나, 패킷 번들의 바이트 크기가 증가하거나, 도착 간격이 짧아지는 등의 특징을 독립적으로 추출하고, 이후 각 특징을 결합하여 지역적 특징으로 모델이 행위를 학습하게 한다. 각 채널별 통계적 특징(바이트 크기, 패킷 개수, IAT)을 독립적으로 처리하여 손실 없이 특화된 패턴을 학습하는 동시에, 이후 단계에서 채널 간 상호작용을 통합적으로 고려한다. 그 결과 세션 내부의 미세한 트래픽 변화—예를 들어 메시지 송수신과 파일 업·다운로드 —을 정밀하게 구분할 수 있으며, 세션 단위 분석의 한계를 보완하여 전체 행위 인식의 정밀도를 향상시킨다.

Ⅳ. 실험 및 결과

본 장에서는 제안한 행위 분석 프레임워크의 성능을 평가하기 위해 WeChat 트래픽을 대상으로 2D CNN과 1D CNN 모델을 각각 학습 및 검증하였다. 모델의 성능 평가는 정확도를 기준으로 수행하였으며, 각 데이터셋은 8:2 비율로 분할하였다.

4.1. 세션 단위 2D CNN 결과

표 2. 세션 단위 2D CNN 분류 정확도 결과
Table 2. Session-level Classification Results

Feature Layer	Accuracy
L3 + L4 + L7	95.22%
L7	93.3%

표 2은 세션 단위 트래픽을 대상으로 2D CNN을 적용한 분류 결과를 나타낸 것이다.
세션 이미지는 28×28 크기로 변환되어 입력되었으며, 모델은 Voice, Video, Others 등 기능별 세션의 구조적 특성을 학습하도록 설계되었다.

그 결과, 2D CNN은 L3와 L4의 헤더 정보를 포함한 경우 약 95%의 분류 정확도를 보였고, 페이로드만 사용하는 경우 93% 수준의 분류 정확도를 보였다.

특히 Voice와 Video 트래픽은 전송 주기, 데이터 방향성, 세션 지속 시간에서 명확한 차이를 보이기 때문에, CNN 기반의 패턴 학습에 유리하게 작용한 것으로 해석된다.

4.2. 패킷 번들 단위 1D CNN 결과

표 3은 Chat/File Transfer 세션의 세부 행위를 구분하기 위해 수행한 1D CNN 기반 분류 결과를 나타낸 것이다. 세션 내 트래픽은 1초 단위의 패킷 번들로 분할되었으며, 각 번들은 송신, 수신, 양방향 트래픽으로 구성된 3채널 입력 구조로 설계되었다.

표 3. 패킷 번들 단위 1D CNN 분류 정확도 및 비교실험
Table 3. Packet-Bundle-level Classification Results

Application	Layers	1D CNN Acc	ActiveTracker Acc
WeChat	L3+L4+L7	97.03	63.25
	L7	95.02	
WhatsApp	L3+L4+L7	90.91	51.05
	L7	93.18	
KakaoTalk	L3+L4+L7	97.67	53.3
	L7	100	

각 채널은 독립적인 Conv1D - MaxPooling 블록을 통해 개별 특징을 추출한 뒤, Flatten 과정을 거쳐 병합(Fusion)된다. 이러한 채널 분리형 구조는 트래픽의 방향성에 따라 서로 다른 전송 패턴을 독립적으로 학습할 수 있도록 하여, 단일 입력 구조 대비 행위 구분에 유리하다. 예를 들어 Chat 세션은 간헐적이고 소규모의 송신 패킷이 주로 발생하는 반면, File Transfer 세션은 일정 시간 동안 대용량의 양방향 데이터가 집중되는 Burst 형태를 보인다. 3채널 구조는 이러한 차이를 각 방향별 특징 공간에서 개별적으로 학습함으로써, 행위 단위의 미세한 전송 패턴을 더욱 정밀하게 포착할 수 있다.

실험 결과, 제안한 1D CNN 모델은 3개의 합성곱층을 사용할 때 평균 97%의 분류 정확도를 달성하였다. 특히 다채널 입력 구조를 적용하지 않은 단일 채널 모델 대비 약 6~7% 향상된 성능을 보였으며, 이는 제안한 구조가 트래픽의 시간적·방향적 특징을 효과적으로 분리하여 학습함으로써 Chat/File Transfer 행위 인식의 정밀도를 향상시켰음을 의미한다.

또한, 방법론의 일반화 성능을 검증하기 위해 데이터셋 Ablation 실험을 수행하였다. 본 방법론은 WeChat과 유사한 트래픽 발생 경향을 보이는 SNS 어플리케이션에 모두 적용이 가능하다. 따라서, 수집 결과 WeChat과 유사한 트래픽 발생 경향을 보이는 WhatsApp과 KakaoTalk 트래픽에도 동일한 1D CNN 구조를 적용한 결과, 두 애플리케이션 모두 90% 이상의 높은 정확도를 보였다.

V. 결 론

본 연구에서는 암호화된 네트워크 환경에서 사용자의 행위를 효과적으로 식별하기 위해, WeChat 트래픽을 대상으로 한 행위 기반 트래픽 분석 프레임워크를 제안하였다.

WeChat은 메시지, 음성·영상 통화, 파일 전송 등 다양한 기능을 통합적으로 제공하는 대표적인 SNS형 애플리케이션으로, 기능별로 상이한 세션 구조와 전송 패턴을 보인다. 이를 반영하기 위해, 본 연구는 세션 단위(2D CNN)과 패킷 번들 단위(1D CNN)의 이중 구조를 설계하여 행위 구분의 정확도를 향상시켰다. 패킷 번들 단위의 1D CNN은 Chat/File Transfer와 같은 유사 세션 간 미세한 시간적 패턴 차이를 효과적으로 학습하였고, 송신·수신·양방향 3채널 구조를 통해 방향성별 특징을 독립적으로 추출함으로써 행위 분류 성능을 향상시켰다. 추가적으로 WhatsApp과 KakaoTalk 데이터셋에 동일한 모델을 적용한 Ablation 실험 결과, 제안된 구조가 특정 서비스에 종속되지 않고 다양한 메신저 트래픽에 일반화될 수 있음을 확인하였다.

향후 연구에서는 더욱 정교한 행위 인식과 실시간 적용성을 높이기 위한 확장 연구가 요구되고, 패킷 번들이라는 개념을 도입하여 1D CNN이 아닌 Transformer 등 기타 딥러닝 모델의 전처리 방식으로 패킷 정확도 뿐만이 아닌 기타 평가 요소들을 적용하여 모델을 평가하여야 한다.

첫째, WeChat의 파일 전송 과정에서 일부 트래픽 구간이 비동기 채널이나 별도 업로드 절차를 통해 전송되는 것으로 추정되며, 이에 대한 네트워크 계층 수준의 추가 분석이 필요하다.

둘째, 세션 구간 정의를 시간 단위에서 Burst 단위로 확장할 경우 Chat/File Transfer 행위 간의 구분 성능이 향상되는 것으로 확인되었으므로, 향후 연구에서는 이러한 동적 분할 기법을 반영할 예정이다.

셋째, 1D CNN의 3채널 구조를 추가적인 통계 지표(예: 패킷 지연, 전송 비율 등)로 확장함으로써 더 세밀한 행위 구분 및 다중 클래스 분류로 발전시킬 수 있을 것이다.

결론적으로, 본 연구는 암호화된 환경에서도 비페이로드 트래픽의 통계적·시간적 패턴만으로 사용자 행위를 정량적으로 식별할 수 있음을 실험적으로 입증하였다.

향후에는 Burst 기반 세션 정의와 다채널 통계 확장을 포함한 고해상도 행위 분석 모델을 구축하여, 서비스별 트래픽 행위 인식의 범용성과 실시간 분석 가능성을 동시에 확보하는 방향으로 발전시킬 예정이다.

References

[1] Guang Cheng and Song Wang, "Traffic classification based on port connection pattern," 2011 International Conference on Computer Science and Service System (CSSS), Nanjing, 2011, pp. 914-917, doi: 10.1109/CSSS.2011.5974374.

[2] M. S. Raza, S. B. A. Kazmi, R. Ali, M. M. Naqvi, H. Fiaz and A. Akram, "High Performance DPI Engine Design for Network Traffic Classification, Metadata Extraction and Data Visualization," 2024 5th International Conference on Advancements in Computational Sciences (ICACS), Lahore, Pakistan, 2024, pp. 1-6, doi: 10.1109/ICACS60934.2024.10473274.

[3] Moore, Andrew & Zuev, Denis. (2005). Internet traffic classification using Bayesian analysis techniques. Sigmetrics Performance Evaluation Review - SIGMETRICS. 33. 50-60. 10.1145/1064212.1064220.

[4] Lotfollahi, Mohammad & Shirali hossein zade, Ramin & Jafari Siavoshani, Mahdi & Saberian, Mohammadsadegh. (2020). Deep Packet: A Novel Approach For Encrypted Traffic Classification Using Deep Learning. Soft Computing. 24. 10.1007/s00500-019-04030-2.

[5] Wei Wang, Ming Zhu, Xuewen Zeng, Xiaozhou Ye and Yiqiang Sheng, "Malware traffic classification using convolutional neural network for representation learning," 2017 International Conference on Information Networking (ICOIN), Da Nang, Vietnam, 2017, pp. 712-717, doi: 10.1109/ICOIN.2017.7899588.

[6] Hwang, R.-H.; Peng, M.-C.; Nguyen, V.-L.; Chang, Y.-L. An LSTM-Based Deep Learning Approach for Classifying Malicious Traffic at

the Packet Level. Appl. Sci. 2019, 9, 3414.
[7] Lin, Xinjie & Xiong, Gang & Gou, Gaopeng & Li, Zhen & Shi, Junzheng & Yu, Jing. (2022). ET-BERT: A Contextualized Datagram Representation with Pre-training Transformers for Encrypted Traffic Classification. 633-642. 10.1145/3485447.3512217.
[8] Li, Ding & Li, Wenzhong & Wang, Xiaoliang & Nguyen, Cam-Tu & Lu, Sanglu. (2020). App Trajectory Recognition over Encrypted Internet Traffic based on Deep Neural Network. Computer Networks. 179. 107372. 10.1016/j.comnet.2020.107372.
[9] Shafiq, Muhammad & Yu, Xiangzhan & Laghari, Asif. (2018). WeChat traffic classification using machine learning algorithms and comparative analysis of datasets. International Journal of Information and Computer Security. 10. 109. 10.1504/IJICS.2018.091467.

김 지 민 (Ji-Min Kim)

2020 ~ 현재 : 고려대학교 컴퓨터융합소프트웨어학과 학사 과정
<관심분야> 네트워크 관리 및 보안, 트래픽 모니터링 및 분석

김 란 아 (Ran-A Kim)

2024 ~ 현재 : 고려대학교 미래모빌리티학과 학사 과정
<관심분야> 네트워크 관리 및 보안, 트래픽 모니터링 및 분석

장 윤 성 (Yoon-Seong Jang)

2023 : 고려대학교 컴퓨터융합소프트웨어학과 학사
2023 ~ 현재 : 고려대학교 컴퓨터정보학과 석/박사 통합과정
<관심분야> 네트워크 트래픽 모니터링, SDN

백 의 준 (Ui-Jun Baek)

2018년 : 고려대학교 컴퓨터정보학과 학사
2025년 : 고려대학교 컴퓨터정보학과 박사
2025년 ~ 현재 : 한국과학기술정보연구원(KISTI) 선임연구원
<관심분야> 블록체인 거래 모니터링, 네트워크 관리 및 보안, 트래픽 모니터링 및 분석

김 명 섭(Myung-Sup Kim)

1998년 : 포항공과대학교 전자계산학과 학사
2000년 : 포항공과대학교 전자계산학과 석사
2004년 : 포항공과대학교 전자계산학과 박사
2006년 : Dept. of ECS, Univ of Toronto Canada
2006년 ~ 현재 : 고려대학교 컴퓨터정보학과 교수
<관심분야> 네트워크 관리 및 보안, 트래픽 모니터링 및 분석, 단일미디어 네트워크