Multi-Input CNN을 활용한 UDP 기반의 암호화 트래픽 분류

박지태, 이민성, 최정우, 이정원*, 김명섭
고려대학교, 닥터소프트*
{pjj5846, min0764, choigoya97, tmskim}@korea.ac.kr, ljwbom@doctorsoft.co.kr*

A UDP based Encrypted Traffic Classification using the Multi-Input CNN

Jee-Tae Park, Min-Seong Lee, Jung-Woo Choi, Jeong-Weon Lee*, Myung-Sup Kim
Korea Univ, Doctorsoft*

요 약

최근 네트워크 기술의 발전과 네트워크 내 발생하는 여러 가지의 보안 이슈로 인해 다양한 응용에서 암호화 트래픽을 사용하는 추세이다. 암호화 기술은 SSL 프로토콜 개발을 시작으로 꾸준히 발전하였으며, 현재는 TLS 1.2가 가장 널리 사용되고 있다. 하지만 기존의 암호화 기술은 특정 공격에 대하여 보안이 취약하며, 연결 속도가 느리다는 문제점이 있다. 이러한 문제점을 해결하기 위해서 구글은 기존의 TCP 기반의 암호화 프로토콜 대신 UDP 기반의 암호화 프로토콜인 QUIC을 개발하여 사용하고 있다. 암호화 트래픽에 대한 연구는 이전부터 활발하게 진행되었지만, 대부분의 연구는 TCP 기반의 암호화 트래픽을 대상으로 수행되어왔다. 따라서 본 논문에서는 TCP 기반의 아닌 UDP 기반의 QUIC를 대상으로 CNN을 활용한 암호화 트래픽 분류 모델을 설계한다. 또한, 설계된 모델을 실제로 수집한 QUIC 트래픽에 적용하여 해당 방법론의 타당성을 검증한다.

Ⅰ. 서 론

네트워크 기술의 발전에 따라 다양한 응용 및 악성행위가 발생하고 있으며, 이에 여러 가지 보안 문제가 발생하였다. 이러한 문제를 해결하기 위해 네트워크 트래픽의 암호화 기술에 대한 연구가 진행되어 왔으며, SSL 프로토콜 개발을 시작으로 꾸준히 발전하고 있다. 현재 개발된 여러 가지 버전의 암호화 프로토콜 중 TLS 1.2가 가장 보편적으로 사용되고 있으며, 기존의 여러 가지 악성행위 및 보안 이슈에 대하여 효과적으로 해결한다.

하지만 TLS 1.2는 보안이 강화 될수록 연결 속도가 느려지며, 특정 공격에 대해서는 취약하다는 문제점이 있다. 또한 HoL(Head of Line) Blocking 이슈와 암호화 되지 않은 Handshake 및 SNI(Server Name Indication) 정보를 통해 해당 패킷에 대한 정보를 유추 할 수 있기 때문에 여전히 보안상 취약점이 존재한다. 이를 해결하기 위해서 구글은 SPDY 프로토콜을 개발하여 많은 문제점을 해결하였지만, 기존 프로토콜과 연동 호환 문제 및 여전히 발생하는 연결 지연에 대한 취약점이 존재한다[1].

이러한 문제를 해결하기 위한 다양한 연구가 진행되었으며, 구글은 2013년 UDP 기반의 암호화 프로토콜 QUIC를 개발하였다. QUIC는 최근 IETF에서 표준화를 진행하였으며, 차세대 웹 통신 프로토콜인 HTTP/3은 하위 계층으로 사용 할 예정이다[1]. UDP 기반의 QUIC는 TCP 기반의 프로토콜에 비해 가볍고, 보안성을 보장하며, 특히 TCP 연결에 비해서 지연 시간을 대폭 줄일 수 있다는 장점이 있다[1]. 이러한 장점으로 QUIC는 이미 구글 크롬 기반의 응용 프로그램과 Youtube 동영상 스트리밍을 포함한 많은 응용에서 사용되고 있으며, 실제로 고려대학교 학내망 네트워크에서 수집한 트래픽 중 약 13% 차지하고 있다. 앞으로도 낮은 지연시간과 원활한 서비스 제공을 요구하는 게임, 화상회의를 포함한 많은 응용에서 QUIC 사용은 점차적으로 늘어날 것으로 보인다.

이 연구는 2020년도 산업통상자원부 및 한국산업기술평가관리원(KEIT) 연구비 지원에 의한 연구임 (No. 20008902, IT비용 최소화를 위한 5채널 탐지기술 기반 SaaS SW Management Platform(SMP) 개발)

암호화 기술의 발전에 따라 암호화 트래픽 양이 크게 증가하였으며, 최근에는 대부분의 응용에서 암호화 트래픽을 사용한다[1,2]. 이러한 추세에 따라 암호화 트래픽 분류에 대한 다양한 연구가 수행되어 왔으며, 대부분의 암호화 트래픽 분류에 대한 연구는 TCP 기반의 암호화 프로토콜을 대상으로 수행되었다[2,3]. 하지만 QUIC의 높은 성능과 프로토콜 표준화 채택 및 HTTP/3에서의 적용을 고려할 때, UDP 기반의 QUIC에 대한 암호화 트래픽 분류 연구가 필요하다. 따라서 본 논문에서는 QUIC 프로토콜을 대상으로 암호화 트래픽 분류 모델을 설계하고, 실제로 QUIC 트래픽을 수집하여 암호화 트래픽 분류 실험을 수행한다.

본 논문의 구성은 본 장의 서론에 이어 2장 본론에서 분류 모델에 대해 설명하고, 3장에서 이에 대한 실험을 수행하며, 4장에서 결론을 제시한다.

Ⅱ. 본론

2장에서는 본 논문에서 제안하는 분류 모델에 대해 설명한다. 제안하는 분류 모델에 대한 구조는 그림 1에 나타나있으며, 트래픽 수집, 전처리 과정, 모델 학습, 모델 검증으로 구성되어 있다.

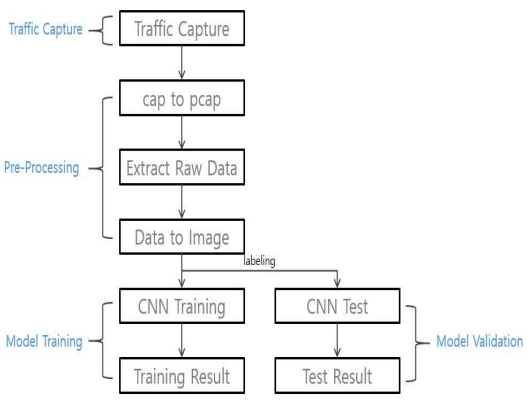

그림 1 CNN 기반 응용 트래픽 분류 모델 구조

먼저 트래픽 수집은 각 응용의 GT(Ground-Truth) 트래픽을 수집하기 위해 Microsoft에서 제공하는 Microsoft Network Monitor를 사용한다. 전처리 과정은 크게 세 단계로 구분되며, 수집 된 .cap 파일을 pcap 파일 포맷으로 변환하고, 이를 플로우 단위의 트래픽 포맷으로 변환한다. QUIC는 플로우 간 처음 연결 시 발생하는 패킷에서 중요한 정보를 포함하기 때문에, 변환 된 플로우의 1~10번째 패킷을 대상으로 헤더를 포함한 패킷의 byte를 추출한다. 추출된 데이터의 각 byte는 0~255 사이의 값을 가지며, 모든 전처리 과정을 거치면 10개의 패킷을 대상으로 28×28 사이즈의 흑백 음영 이미지가 도출된다.

모델 학습 단계에서는 변환된 응용 트래픽 이미지 파일을 대상으로 학습하며, 수집 된 응용에 따라 labeling을 통해 응용을 구분한다. 본 논문에서는 전처리 과정에서 생성된 10장의 흑백 음영 트래픽 이미지가 입력으로 들어가는 다중 입력 CNN 모델을 사용하며, 모델의 전반적인 구조는 그림 2에 나타나있다. 하나의 CNN 모델은 Input Layer로부터 하나의 트래픽 이미지를 입력으로 받아, Convolution, Max Pooling 과정을 거친다. 각각의 모델에서 나온 결과를 하나로 합친 후, softmax를 사용하는 Fully Connected Layer를 거친다.

마지막으로 모델 검증 단계에서는 선정한 모델을 대상으로 학습에 사용되지 않은 데이터에 대한 분류를 수행하고, 분류 결과와 labeling과 비교하여 분류 정확도를 도출한다.

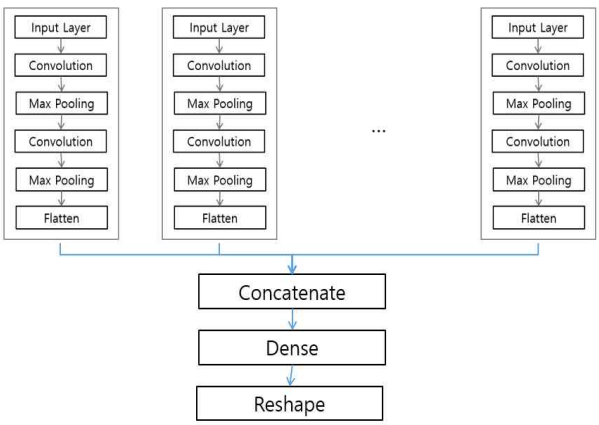

그림 2 다중 입력 CNN 모델 구조

Ⅲ. 실험

3장 실험에서는 제안한 CNN 기반 분류 모델을 검증하기 위해 실제로 수집한 UDP 기반의 트래픽을 대상으로 실험을 진행하며, 실험에 사용한 응용 트래픽에 대한 정보는 표 1에 나타나있다.

표 1 응용 트래픽 정보

응용 트래픽	프로토콜	플로우	패킷	바이트
Google Meet	QUIC (UDP based)	524	90,254	102,086,415
Google Drive		611	87,403	86,261,402
Youtube		338	54,607	91,840,005
Youtube Music		462	162,232	190,028,457

실험은 4가지 UDP 기반의 응용(Google Meet, Google Drive, Youtube, Youtube Music)을 대상으로 진행하며, 실험에 사용 한 응용 트래픽 정보는 표 1에 나타나있다. 수집 된 트래픽은 모두 QUIC 프로토콜이며, 기본적으로 UDP 443포트를 사용한다.

실험에 사용한 모델의 hyper-parameter는 각 모델에 따라 다양하게 설정하였으며, train set은 전체 데이터의 60%, test set은 40%로 지정하였다. 표 2는 hyper-parameter의 조합으로 생성된 여러 모델을 나타낸다. 표 2의 4가지 모델을 대상으로 학습을 수행하고, 이를 기반으로 분류 검증 실험을 수행한다. 각각의 학습 모델에 대한 학습 및 검증 결과는 표 3에 나타나있다.

표 2 선정 된 학습 모델

Model	Learning Method	Activation Function	Pooling
1	Multi-Input CNN	ReLU	Max Pooling
2		Tanh	Max Pooling
3		Sigmoid	Max Pooling
4		ReLU	Average Pooling

각 모델에 대한 학습 수는 100,000번이며, Learning Rate는 0.0001로 설정하였다. 모델의 학습 정확도는 75~96%, 가장 높은 학습 정확도는 97%로 타나났으며, 검증 정확도는 85~90%, 가장 높은 검증 정확도는 90%로 나타났다. 각 모델 중에서 가장 좋은 성능을 보이는 모델은 ReLU, Max Pooling을 사용하는 모델이다.

표 3 응용 트래픽 분류 실험 결과

Model	Epoch	Learning Rate	Train Accuracy	Test Accuracy
1	100,000	0.0001	97.01%	89.63%
2			79.49%`	51.18%
3			78.59%	50.72%
4			77.11%	48.26%

Ⅳ. 결론

본 논문에서는 TCP 기반의 암호화 트래픽의 문제점과 UDP 기반의 암호화 트래픽 분류 연구 필요성에 대해 언급하였다. UDP 기반의 암호화 프로토콜을 대상으로 트래픽 분류 모델을 설계하고, 네트워크에서 실제로 발생하는 QUIC 트래픽을 수집하여 실험을 진행하였다. 수집한 QUIC 응용 트래픽은 4가지이며, 다중 입력 CNN 모델을 사용하여 분류 하였다. hyper-parameter의 조합에 따라 여러 가지 학습 모델을 생성 할 수 있지만, 본 논문에서는 표 2의 4가지 학습 모델을 사용한다. 전체 모델 중 ReLU, Max Pooling을 사용한 모델에서 학습 정확도 97%, 검증 정확도는 90%로 가장 높은 성능을 보인다. 향후 연구로 더 많은 종류의 QUIC 트래픽을 대상으로 실험 할 예정이며, CNN 모델뿐만 아니라 다른 딥러닝 모델을 사용하여 분류 검증 성능을 높일 예정이다.

참 고 문 헌

[1] 남혜빈, 정중화, 최동규, 고석주. “웹 및 스트리밍 서비스에 대한 QUIC 프로토콜 성능 분석”. 정보처리학회논문지. 컴퓨터 및 통신시스템, 10(5), 137-144. 2021

[2] 김성민, 박준상, 윤성호, 김종현, 최선오, 김명섭. “SSL/TLS 기반 암호화 트래픽의 서비스 식별 방법.”, 한국통신학회논문지, 40(11), 2160-2168, 2015

[3] 전덕조, 박동규. “머신 러닝 (Machine Learning) 기법을 활용한 암호화된 TLS 트래픽내 악성코드 탐지 기법”. 한국정보기술학회논문지, 19(10), 125-136. 2021