트래픽 플로우 및 딥러닝 기반의 프로토콜 분류 방법론

박예진[1], 조영필[2]
[1]한양대학교 컴퓨터소프트웨어학과 (미래자동차-SW 융합전공) 석박통합과정
[2]한양대학교 컴퓨터소프트웨어학과 교수

pkyj09029@hanyang.ac.kr, ypcho@hanyang.ac.kr

Protocol Classification Based on Traffic Flow and Deep Learning

Ye-Jin Park[1], Yeong-Pil Cho[2]
[1] Dept. of Computer and Software (Automotive-Computer Convergence), Han-Yang University
[2] Dept. of Computer Science, Han-Yang University

요 약

본 논문은 현대 사회에서 급증하는 VPN의 악용 가능성을 인지하고 VPN과 Non-VPN 트래픽 구별의 중요도를 강조한다. 전통적인 포트 기반 분류와 패킷 분석 접근법의 한계를 넘어서기 위해 트래픽 플로우 특징과 인공지능(AI) 기술을 결합하여 VPN과 Non-VPN 프로토콜을 구별하는 새로운 방법을 제안한다. 직접 수집한 패킷 데이터셋을 사용하여 트래픽 플로우 특징을 추출하고, 패킷의 페이로드와 결합해 이미지를 생성한다. 이를 CNN 모델에 적용함으로써 높은 정확도로 프로토콜을 구별한다. 실험 결과, 제안된 방법은 99.71%의 높은 정확도를 달성하여 트래픽 분류 및 네트워크 보안 강화에 기여할 수 있는 방법론임을 입증한다.

1. 서론

현대 사회에서 인터넷의 역할은 매우 중요하며, 그 사용량은 지속적으로 증가하고 있다. 이러한 상황에서 네트워크 보안과 관리는 더욱 중요한 과제가 되었다. 특히 코로나19 바이러스 감염병 유행으로 인해 원격 근무가 증가하면서, 가상 사설 네트워크(VPN) 사용자가 급격히 늘어났다. VPN은 데이터 전송 과정에서의 보안과 개인 정보 보호를 위해 사용되지만, 동시에 이를 악용한 사이버 공격과 데이터 유출의 위험 또한 증가시킨다. 이에 따라 VPN과 Non-VPN 프로토콜을 효과적으로 구별하는 방법에 대한 수요가 급증했다.

전통적인 네트워크 프로토콜 분류 방법은 포트 기반 접근법과 패킷 분석 접근법 등이 있지만, 동적으로 포트 번호를 할당하거나 패킷을 암호화하는 등의 다양한 우회 방법이 발달하며 정확도가 크게 감소하였다. 이에 따라, 트래픽 플로우 분석을 통한 프로토콜 분류와 딥러닝 모델 기반의 분류 방법이 새롭게 제안되었다.

본 논문은 최근에 제시된 두 방안을 결합하여 더 높은 정확도로 VPN과 Non-VPN 프로토콜을 구별하는 것을 목표로 한다. 네트워크 트래픽 플로우 특징과 페이로드를 딥러닝 모델에 함께 학습시켜 99.71%의 정확도를 달성했다.

2. 관련연구

트래픽 분류를 위한 고전적인 방법으로 포트 기반 접근법과 패킷 분석 접근법이 있다.[1][2] 간단한 구현으로 쉽게 사용되어 온 방법들이지만 둘 이상의 포트를 사용하는 프로토콜이나 암호화되어 패킷의 내용을 읽을 수 없는 경우 적용할 수 없다는 큰 단점이 존재한다.

최근의 네트워크 프로토콜 분류 연구는 암호화된 패킷과 동적 포트 할당 등 다양한 우회 방법에 유연하게 대처할 수 있는 방향으로 발전하고 있다.

VPN과 TOR 네트워크 프로토콜 분류를 위해 트래픽 플로우 특징을 추출한 뒤 MLP(Multiple-Layer Perceptron)와 LSTM(Long Short-Term Memory)과 같은 인공지능 모델을 적용한 연구가 최대 96%의 정확도를 기록했다.[3] 암호화된 네트워크 트래픽 중 VPN과

Non-VPN 프로토콜 분류를 위해 CNN(Convolutional Neural Network) 딥러닝 모델을 적용한 결과 92.92%의 정확도를 달성했다.[4]

3. 실험 설계

VPN과 Non-VPN 프로토콜을 정확하게 분류하기 위해 트래픽 플로우 특징과 패킷의 페이로드를 결합하여 이미지를 생성하고, CNN 딥러닝 모델을 적용하는 방법을 제안한다.

3.1. 데이터셋

본 논문에서 사용된 데이터셋은 모두 직접 수집한 패킷으로 암호화 여부와 관계없이 프로토콜별로 분류한다. 유료 개인용 가상 사설망 서비스인 NordVPN을 통해 VPN 프로토콜 중 OpenVPN과 NordLynx를 수집했다.[5] NordLynk는 기존의 VPN 프로토콜인 WireGuard를 기반으로 구축된 기술로, 본 논문에서는 WireGuard라고 분류한다. OpenVPN은 TCP/UDP의 구분 없이 수집되었다. SSTP는 무료로 제공되는 VPN Gate를 통해 수집했다.[6] Non-VPN 데이터 수집은 통상적으로 발생하는 패킷을 사용해도 무방하나 VPN 프로토콜과 유사도가 높아 실제 인터넷 환경에서 혼동되기 쉬운 프로토콜을 대상으로 했다. QUIC, SFTP와 SSH 같이 TLS(Transport Layer Security)가 적용된 프로토콜을 Non-VPN으로 하나의 카테고리로 묶어 실험을 진행한다.

<표 1> 프로토콜 데이터셋

Protocol	Train	Test	Total
OpenVPN	13805	3453	17258
WireGuard	261435	65359	326794
SSTP	794879	198721	993600
Non-VPN	94267	23572	117839

3.2. 트래픽 플로우 특징 추출 및 이미지 생성

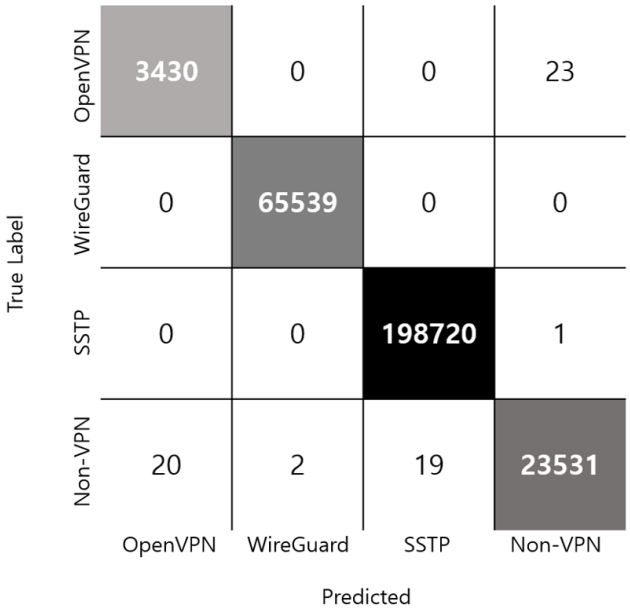
수집한 패킷들을 네트워크 트래픽 플로우로 변환하고 특징을 추출하기 위해 자바 오픈소스 툴인 CIC-Flowmeter를 사용한다.[7]. 추출되는 다양한 특징 중 학습의 편향에 영향을 주는 IP 주소와 포트 번호는 제외한다. 먼저 XGBoost 알고리즘으로 프로토콜을 학습하고, 중요도에 따라 특징의 순위를 매긴다. 본 실험에 사용된 상위 5개의 특징은 <표 2>와 같다. 각각의 특징마다 고정된 길이를 가질 수 있게 자르거나 남은 바이트 수만큼 0을 채워 넣어주며 결합한다. 결합된 최종 특징에 헤더를 제외한 페이로드를 부착한다. 패킷의 헤더를 제거하는 이유도 송수신 IP와 포트, 패킷 길이 등으로 인한 편향을 막기 위해서다. 페이로드의 경우에도 마찬가지로 공통된 크기의 이미지를 생성하기 위해 1024 바이트에 맞춰 남은 바이트 수만큼 0을 채워 넣었다. 생성된 이미지는 8:2의 비율로 CNN 모델에 학습 혹은 평가되었다.

<표 2> 중요도 순위에 따른 트래픽 플로우 특징

1	The total number of bytes sent in initial window in the backward direction
2	Number of packets with PUSH
3	Maximum size of packet in forward direction
4	Number of flow bytes per second
5	Duration of the flow in Microsecond

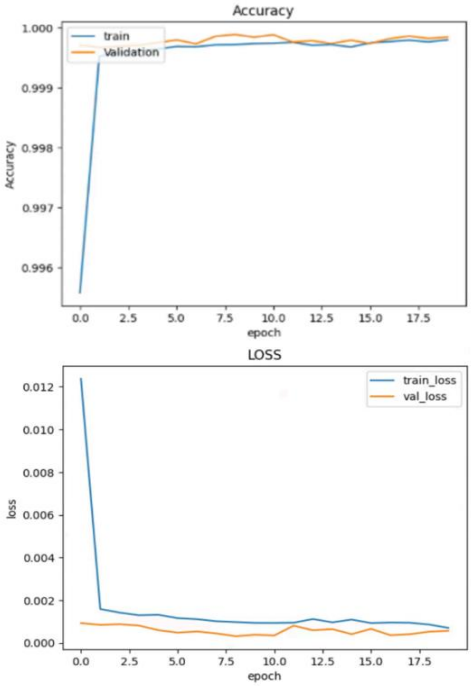
4. 실험 결과

최종적으로 Precision, Recall, F1-Score의 값이 모두 동일하게 0.9997을 기록했다. (그림 1)을 보면 많은 경우에 대해 정확한 분류가 일어났다. 프로토콜별 판정 정확도를 살펴보면 OpenVPN은 99.33%, WireGuard는 100%, SSTP는 99.99%, 마지막으로 Non-VPN은 99.82%의 정확도를 자랑한다. (그림 2)에 따르면 전체적인 accuracy는 0.9971을, loss는 0.00181를 기록했다.



(그림 1) VPN/Non-VPN 프로토콜 분류 결과

다만, 수집한 데이터셋의 수가 VPN 프로토콜에 편향되어 있어 현재 결과를 완전히 신뢰할 수는 없다. 실제 인터넷 환경에서는 Non-VPN 프로토콜이 VPN 프로토콜에 비해 훨씬 많을 것이라 예상되기 때문에 추후에 데이터셋을 조정해 다시 실험해보려 한다.



(그림 2) accuracy와 loss 측정 결과

5. 결론

본 논문에서는 VPN의 악용 가능성을 인지하고 VPN과 Non-VPN 프로토콜을 효과적으로 구별하는 새로운 방법을 제안한다. 트래픽 플로우 특징과 패킷의 페이로드를 결합하여 딥러닝 모델에 학습하면 99.71%의 정확도로 VPN과 Non-VPN 프로토콜을 구분할 수 있다. 추후에는 실제와 가까운 환경을 구축하고 실험을 계속하며 신뢰도를 보완해가려고 한다.

이 논문은 과학기술정보통신부의 재원으로 정보통신기획평가원(No. 2020-0-01840, 스마트폰의 내부데이터 접근 및 보호 기술 분석)과 한국연구재단(No. NRF-2022R1A4A1032361, Processing-in-Memory 보안 기술 개발)의 지원을 받아 수행된 연구임

참고문헌

[1] Velan, P., Čermák, M., Čeleda, P., & Drašar, M. (2015). A survey of methods for encrypted traffic classification and analysis. International Journal of Network Management, 25(5), 355-374.

[2] IANA port number list, Available: http://www.iana.org/assignments/service-names-prt-numbers/service-names-port-numbers.xml

[3] Islam, F. U., Liu, G., Zhai, J., & Liu, W. (2021). VoIP traffic detection in tunneled and anonymous networks using deep learning. IEEE Access, 9, 59783-59799.

[4] Islam, F. U., Liu, G., Zhai, J., & Liu, W. (2021). VoIP traffic detection in tunneled and anonymous networks using deep learning. IEEE Access, 9, 59783-59799.

[5] The best online VPN service for speed | NordVPN. (2024, April 9). NordVPN. https://nordvpn.com/

[6] VPN Gate - Public Free VPN Cloud by Univ of Tsukuba, Japan. (n.d.). https://www.vpngate.net/

[7] Lashkari, A. H., Gil, G. D., Mamun, M. S. I., & Ghorbani, A. A. (2017, February). Characterization of tor traffic using time based features. In International Conference on Information Systems Security and Privacy (Vol. 2, pp. 253-262). SciTePress.