AI 기반 암호화 트래픽 분석 기술 동향

김찬형, 윤종희
영남대학교 컴퓨터공학과(석사과정, 교수)
qhfrha@yu.ac.kr, youn@yu.ac.kr

AI-Based encrypted traffic analysis technology trends

Chan-Hyung Kim, Jonghee Youn
Dept. of Computer Engineering, Yeungnam University

요 약

개인정보 및 네트워크 데이터 보호 등의 목적으로 암호화 통신이 보급됨에 따라 암호화 통신 바탕의 IoT기반 인프라 및 서비스가 급속히 구축, 확산되고 있다. 이러한 암호화 통신은 기존 네트워크 장비로는 내용 확인이 불가능하다는 점을 악용하여 악성코드를 은닉하고, 탐지기법을 우회하기 위한 수단으로 사용하는 사례가 꾸준히 발생하고 있다. 암호화 트래픽 분석 기술이란 암호화 통신에서 발생한 트래픽을 해독하지 않고 분석하는 기술로 암호화 통신을 악용한 사례에 대응하기 위한 수단으로써 그 필요성이 대두되고 있다. 본 논문에서는 암호화 통신과 암호화 트래픽에 대해 설명하고 암호화 트래픽 분석 기술의 연구 동향에 대해 분석한다.

1. 서론

암호화 통신 중심의 네트워크로 패러다임이 전환됨에 따라 전 세계적으로 암호화 통신 바탕의 IoT 기반 인프라 및 서비스가 급속히 구축, 확산되고 있다. 이러한 암호화 통신은 기존 네트워크 장비로는 내용 확인이 불가능하다.

현재 이러한 네트워크 보안 사각지대를 노리는 악성행위 사례가 계속해서 증가하고 있다. 그에 따라 이를 방지하기 위한 암호화 트래픽 분석 기술의 중요성이 대두되고 있으며 다양한 연구가 활발히 진행중이다.

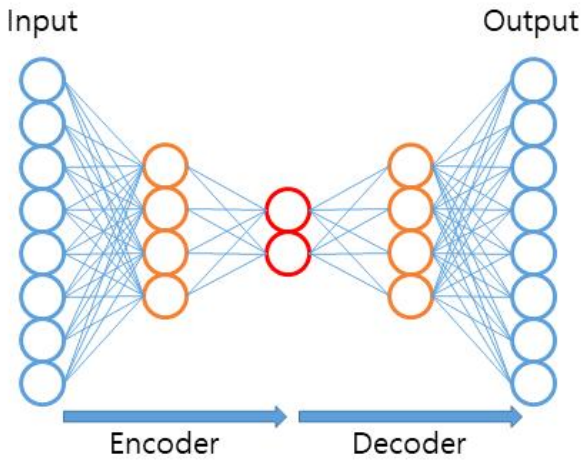
본 논문에서는 이러한 암호화 트래픽 분석 기술 중 AI 기반 암호화 트래픽 분석 기술 연구들을 조사 및 분석하여 기술 동향을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 배경지식에 대하여 설명하고, 3장에서는 연구 동향에 대하여 설명한다. 마지막으로 4장에서 결론을 기술한다.

2. 배경지식

암호화 통신이란 TLS/SSL과 같은 네트워크 보안 프로토콜이 적용되어 이루어지는 통신을 의미한다. 초기 암호화 통신의 경우 그 내용 확인이 불가능하다는 점을 활용하여 개인정보 및 네트워크 데이터 보호 등의 목적으로 보급 되었으나, 이를 악용하여 악성코드 유포, 내부 정보 유출 등에 악용되는 사례가 계속해서 발생하고 있다.

암호화 트래픽 분석 기술이란 이러한 암호화된 데이터를 해독하지 않고 네트워크 트래픽을 분석하여 정보를 추출하는 기술이다. 악성행위를 암호화 통신에 은닉할 경우 기존의 네트워크 장비로는 확인이 불가하기 때문에 이러한 암호화 트래픽 분석 기술의 중요성이 커지고 있다.



(그림 1) 오토인코더 구조도

오토인코더란 비지도 학습의 일종으로 데이터 압축, 차원 축소, 잡음 제거 등에 사용된다. 그림 1은 오토인코더의 전체적인 구조를 간단하게 나타낸 그림이다. 인코더를 통해 입력 데이터를 압축한 후 이를 다시 디코더를 통해 본래의 형태로 복원하는 구조로 되어있다.

3. 암호화 트래픽 분석 기술 연구 동향

Y Yang [1]등은 암호화 트래픽이 가장 많이 발생한 웹 사이트 중 50가지를 선별하여 이를 다시 분류하는 실험을 진행하였다. 해당 연구는 트래픽 분류를 위해 구별 가능한 특징을 추출하는 오토인코더 모델과 트래픽을 2차원 이미지로 나태내어 학습하는 CNN 모델을 제안하였으며, 이를 Naive Bayes, Logistic Regression 등 총 5가지의 모델과 성능을 비교하였다. 해당 논문에서 제시한 2가지 모델 중 오토인코더 모델의 경우 일부 기존 모델들에 비해 낮은 성능을 보여주는 경우가 존재했으나, CNN 모델의 경우 모든 부분에서 기존 모델들보다 성능이 뛰어났음을 주장한다.

J Cui [2]등은 FlowSpectrum[3]을 활용해 암호화 트래픽을 분류하는 모델인 Semi-2DCAE를 제시한다. Semi-2DCAE 모델은 CNN과 오토인코더를 결합한 모델로 암호화 트래픽으로부터 생성된 FlowSpectrum을 분석하여 이를 분류하는데 사용된다. 오토인코더를 통해 특징 추출 단계에서 사람의 개입을 최소화하였고, 구별 가능한 특징을 추출하여 구별 성능을 높였다. 해당 논문은 기존에 제시된 두 모델 Semi-AE, Semi-1DCAE와의 성능 비교를 통해 Semi-2DCAE의 성능이 개선되었음을 주장한다.

J Holland 등[4]은 nPrint를 활용한 자동화된 트래픽 분석에 대한 새로운 방향성을 제시한다. nPrint란 자동화된 트래픽 분석을 위한 도구이다. nPrint를 통해 생성된 표준화된 네트워크 트래픽 표현은 패킷의 종류에 상관없이 동일한 수의 특징으로 표현되고 각 특징이 동일한 의미를 가지도록 정렬되어 있다. nPrintML은 이러한 표준화된 네트워크 트래픽 표현과 AutoML을 결합한 자동화된 트래픽 분석 시스템이다. nPrint로 통일된 형태의 표현을 분석하기 때문에 패킷의 종류에 관계없이 자동화된 분석이 가능하며, 알고리즘 선택 및 튜닝까지의 과정을 자동화한 AutoML과 결합하여 사람의 개입을 최소화하였다.

4. 결론

본 논문에서는 암호화 트래픽 기반 악성행위를 탐지하기 위한 AI 기반 암호화 트래픽 분석 기술 관련 연구들을 조사하였다. 그 결과, 오토인코더를 활용하여 구별 가능한 특징을 추출하는 모델과 트래픽을 2차원 이미지로 나타내어 학습시키는 CNN 모델을 제시한 논문[1], 암호화 트래픽으로부터 생성된 FlowSpectrum을 활용하여 이를 분류하는 Semi-2DCAE 모델을 제시한 논문[2], 새로운 형태의 트래픽 표현인 nPrint를 활용한 자동화된 트래픽 분류 시스템 nPrintML을 제시한 논문[4] 등이 있었다.

이 중 [1], [2]의 경우 오토인코더를 활용하여 특징 추출을 하고, 암호화 트래픽을 각각 2차원 이미지나 FlowSpectrum으로 나타내어 분류하는 모델을 제시하였으며, [4]의 경우 통일된 형태인 nPrint와 알고리즘 선택 및 튜닝을 자동화한 AutoML에 결합한 모델을 제시하고 있다. [1], [2], [4] 모두 오토인코더나 AutoML을 활용하여 사람의 개입을 최소화하는 방향으로 연구되었다는 공통점이 있었다.

암호화 통신 중심의 네트워크로 패러다임이 전환됨에 따라 사이버공격 행위는 악성코드를 은닉하고, 탐지기법을 우회하기 위한 수단으로 암호화 통신을 악용하는 방향으로 변해가고 있다.

따라서, 암호화 통신을 활용한 대국민 서비스의 안전성·보안성 확보를 위해 암호화 트래픽 기반 악성행위의 대응 필요성이 대두되고 있으며, 이를 위해 암호화 트래픽 분석 기술에 대한 추가적인 연구가 필요할 것으로 사료된다.

참고문헌

[1] Y. Yang, C. Kang, G. Gou, Z. Li and G. Xiong, "TLS/SSL Encrypted Traffic Classification with AutoEncoder and Convolutional Neural Network," 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Exeter, UK, 2018, pp. 362-369

[2] 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.
[3] Luming Yang, Shaojing Fu, Xuyun Zhang, Shi ze Guo, Yongjun Wang, and Chi Yang. 2022. Flo wSpectrum: a concrete characterization scheme of network traffic behavior for anomaly detection. W orld Wide Web 25, 5 (Sep 2022)
[4] Jordan Holland, Paul Schmitt, Nick Feamster, and Prateek Mittal. 2021. New Directions in Auto mated Traffic Analysis. In Proceedings of the 202 1 ACM SIGSAC Conference on Computer and Co mmunications Security (CCS '21). Association for Computing Machinery, New York, NY, USA, 3366 - 3383.