머신러닝 기반 안드로이드 멀웨어 탐지 기술 동향 분석

김가겸, 이연준*
한양대학교 컴퓨터공학과 바이오인공지능 융합전공

icntvk@hanyang.ac.kr, *yeonjoonlee@hanyang.ac.kr

A Survey on Android Malware Detection Technology Based on Machine Learning

Kim Ga Gyeom, Lee Yeon Joon*
Major in Bio Artificial Intelligence, Department of Computer Science and Engineering,
Hanyang University.

요 약

전 세계에서 발생하는 웹 트래픽중 50% 이상은 모바일 기기에서 발생하며 그중 안드로이드 OS는 모바일 기기의 OS 시장에서 가장 높은 점유율을 가지고 있다. 이는 악의적인 행동을 하고자 하는 사이버 범죄자들이 주요 타겟으로 삼는 원인이 된다. 현재 안드로이드 OS를 대상으로 한 수많은 멀웨어 프로그램들이 개발되고 있으며 안드로이드 시장에서 멀웨어 탐지는 중요한 과제중 하나이다. 이러한 멀웨어를 탐지하기 위해 지금까지 다양한 연구가 진행되어 왔으나 전통적인 멀웨어 탐지 연구들은 난독화 등의 다양한 탐지 회피 기술들로 인하여 탐지 정확도가 떨어지는 한계점이 존재한다. 본 논문에서는 이러한 한계점을 극복하기 위하여 멀웨어 및 정상 애플리케이션들의 특징을 학습하여 멀웨어를 탐지하는 머신러닝 기반 안드로이드 멀웨어 탐지 기술에 대한 분석을 진행한다.

Ⅰ. 서 론

오늘날 전 세계에서 발생하는 웹 트래픽 중 50% [1] 이상은 모바일기기에서 발생하고 있으며 모바일 기기의 OS 시장에서 안드로이드 OS 는 70% 이상의 높은 점유율을 가지고 있다 [2]. 이러한 높은 점유율로 인하여 악의적인 행동을 하고자 하는 사이버 범죄자들은 안드로이드 OS 를 타겟으로 다양한 멀웨어 프로그램을 개발하고 있으며 안드로이드 시장에서 이러한 멀웨어를 탐지하는 것은 중요 과제 중 하나로 자리잡고 있다.

안드로이드 시장에서 멀웨어를 탐지하기 위한 다양한 연구가 진행되어 왔으나 코드 분석을 통한 전통적인 정적 탐지 방법은 코드의 난독화, 동적 코드 로딩, 암호화, 에뮬레이터 탐지 등 다양한 보호 및 회피 기술에 취약하다. 이러한 취약점을 극복하기 위하여 멀웨어의 권한 및 동작의 특징을 추출하여 멀웨어를 식별하는 머신러닝 기반 멀웨어 탐지 기술들에 대한 연구가 진행되고 있다.

본 논문에서는 안드로이드 OS 를 대상으로한 멀웨어들을 식별하기 위해 애플리케이션의 정적, 동적 특징 등을 사용한 머신러닝 기반 안드로이드 멀웨어 탐지 기술들의 동향을 분석한다.

Ⅱ. 머신러닝 기반 안드로이드 멀웨어 탐지 기술

머신러닝 기반 멀웨어 탐지기술은 멀웨어의 다양한 특징을 추출 후 학습하여 멀웨어를 식별하는 것 을 목표로 한다. 이를 위해 멀웨어의 코드 및 권한 정보등 정적인 특징을 추출하는 정적 분석 방법과 네트워크 트래픽 등의 프로그램 실행으로 얻을 수 있는 동적인 특징을 추출하는 동적 분석 방법 그리고 정적 분석과 동적 분석을 혼합하여 사용하는 하이브리드 분석 방법 등이 존재한다.

2.1 머신러닝 기반 정적 분석 방법

기존의 정적 분석 방법의 경우 일반적인 동적 분석 방법에 비하여 코드 커버리지가 넓으며 오버헤드가 적다는 장점을 지니고 있다. 그러나 기존 정적 코드 분석 탐지 방법의 경우 넓은 코드 커버리지로 인하여 실제 환경에서 실행이 불가능한 경우도 실행이 가능하다고 판단하는 등 많은 수의 오탐지가 발생할 위험이 존재하며 이는 새로 개발되는 멀웨어 프로그램들이 탐지 기술을 회피할 수 있는 하나의 방법이 될 수 있다. 이러한 문제를 해결하기 위하여 본 논문에서 소개할 머신러닝 기반 정적 분석 방법들은 이러한 오탐지를 줄이기 위하여 다양한 정적 특징을 사용한 멀웨어 탐지 연구를 진행하였다. [3] 은 멀웨어를 효과적으로 탐지하기 위하여 최소한의 권한만을 사용하여 탐지 정확도 향상 및 분석 속도를 감소시키고자 했다. 이를 위해 반드시 필요한 권한을 분석하는 작업(INTERNET 권한과 같이 정상 및 멀웨어 에서 공통으로 사용되는 권한의 중요도값 감소, 적은 수의 멀웨어에서 사용되는 권한은 탐지에서 제외 등)을 진행하였으며 기존에 방법들이 분석에 사용한 권한 목록을 기준으로 84% 감소시켰으며 이는 Google 에서 위험한 권한이라 판단한 24 개 보다 더 적은 22 개의 권한만을 사용하여 분석이 가능하며 기존 분석 방법과 비교하여 탐지 정확도 향상과 분석 시간을 줄일 수 있었다.

[4] 의 경우 오탐지가 발생하는 원인은 멀웨어와 정상 애플리케이션이 많은 공통적인 속성을 공유하기 때문이며 이를 효과적으로 분류를 하기 위해 문자열, 메소드의 Opcode, API, 애플리케이션 구성요소(Activity, Service 등)등의 특징을 추출하였으며 2 가지 방식 (존재기반, 유사성기반)으로 특징 백터를 생성하여 Android 멀웨어 탐지 분야에서 최초로 멀티모델 딥러닝 방식을 사용하여 정확도를 향상시켰다.

2.2 머신러닝 기반 동적 분석 방법

정적 분석방법은 난독화 및 런타임시 동적으로 클래스를 로드하거나 멀웨어를 다운받는 등 애플래케이션 실행시 멀웨어의 특징이 발견되는 경우 탐지가 어렵다는 한계점이 존재한다. 이러한 한계점을 극복하기 위하여 실제 런타임시 발생하는 데이터의 특징을 학습하는 머신러닝

기반 동적 분석 연구가 진행되고 있다. 본 논문에서 소개하는 머신러닝 기반 동적 분석 방법은 멀웨어의 다양한 동적 데이터 특징을 추출하여 멀웨어를 탐지 정확도를 향상시키고자 한다. 동적 분석 방법에서는 기본적으로 네트워크 트래픽의 특징을 사용하는 방식을 선호하며 멀웨어와 정상 애플리케이션의 트래픽을 분석하여 멀웨어를 탐지하는 연구가 주로 진행되고 있다.

[5],[6] 은 네트워크 트래픽 데이터의 송신 IP, 수신 IP, 송신 포트번호, 수신 포트번호, 프로토콜 정보를 사용하여 멀웨어 탐지를 진행하였다. 이 둘은 각자 다른 방식의 머신러닝 방법을 사용하여 멀웨어 탐지를 진행하고자 했다. [5]는 의사결정 트리(DT), 랜덤 포레스트(RF) 모델, 1D-CNN 등 다양한 모델을 사용하여 학습을 진행하고 그중 RF 모델이 가장 높은 정확도로 멀웨어 탐지에 성공하였다. [6]은 CNN(Convolution Neural Network)과 LSTM(Long-Short Term Memory) 아키텍처를 결합한 CNN-LSTM 모델을 사용하여 멀웨어 탐지에 성공하였다. 위 두가지 사례를 통하여 추출한 데이터 뿐 아니라 학습하는 알고리즘 또한 탐지 정확도에 영향을 미친다는 것을 알 수 있다.

[7] 은 효율적인 데이터 분석을 위해 분석할 트래픽 데이터의 최소화를 위해 Information Gain 과 Chi-Square Test 와 같은 통계 기술을 사용하여 각 트래픽 특징 별 중요도를 분석한다. 트래픽의 본 연구의 분석결과 트래픽의 특징 중 상위 9 개의 특징을 사용하여 학습할 경우 전체 트래픽 특징을 사용하는 것 보다 훈련 시간은 50%, 테스트 시간은 30% 감소하여 기존 연구보다 효율적인 탐지가 가능하다는 가능성을 보여준다.

[8] 은 기존 연구들로는 식별이 어려운 복잡한 난독화가 적용된 멀웨어를 탐지하고자 런타임시 생성되는 네트워크 트래픽 및 시스템 호출 추적 정보, 바인더 분석 정보 등 복합적인 특징을 추출하여 학습을 진행한다. 실험결과 난독화된 애플리케이션 대상으로 기존 연구들 보다 더 높은 정확도로 멀웨어 탐지를 성공적으로 수행하였다.

2.3 머신러닝 기반 하이브리드 분석 방법

정적 분석 방법은 런타임시 멀웨어 프로그램 특징이 식별 될 경우, 동적 분석은 멀웨어가 네트워크를 사용하지 않을 경우 탐지가 여럽다는 단점이 존재한다 [9]. 하이브리드 분석 방법은 이러한 단점들을 보안하기 위하여 정적, 동적 분석을 모두 활용하는 하이브리드 분석 방법을 제안한다.

[9] 는 정적 분석 정보와 동적 분석 정보를 결합하여 멀웨어를 탐지하는 최초의 모델이다. 본 논문에서는 정적 분석과 동적 분석에서 멀웨어 탐지에 주로 사용되는 대표적인 특징인 권한 정보와 네트워크 트래픽 정보를 사용하여 멀웨어를 식별하고자 한다. 해당 연구에서는 [7]에서 사용한 네트워크 트래픽 특징의 상위 9 가지 특징과 정적 분석 방법의 권한 특징 정보를 복합적으로 사용하여 멀웨어 탐지율을 향상시켰다.

[10] 은 정적 분석과 동적분석의 탐지 정확도를 향상시키기 위하여 권한 정보, API 호출 특징 정보, 인텐트 필터, 등 다양한 정적 분석 정보와, 시스템 호출, 바인더 호출 등의 동적 정보를 사용하여 다양한 알고리즘으로 학습을 진행한다. 그중 GB 알고리즘을 사용했을 경우 가장 빠른 탐지 속도와 높은 정확도로 멀웨어 탐지를 성공하였다.

Ⅲ. 결론

본 논문에서는 다양한 머신러닝 기반 안드로이드 멀웨어 탐지 연구들에 대하여 분석을 진행하였다. 이러한 연구들이 사용한 분석방법 및 학습에 사용하기위해 추출한 프로그램 특징들은 안드로이드에서의 멀웨어 탐지 뿐 아니라 네트워크 특징 분석, 프로토콜 식별, 프로그램 식별, 클론 앱 탐지 등 다양한 분야의 연구에서 응용이 가능할 것으로 기대된다.

ACKNOWLEDGMENT

이 논문은 2022 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(NRF-2022R1F1A1074999)을 받아 수행된 연구임

참 고 문 헌

[1]https://www.statista.com/statistics/277125/share-of-website-traffic-coming-from-mobile-devices

[2] https://gs.statcounter.com/os-market-share/mobile/worldwide

[3] Li, Jin, et al. "Significant permission identification for machine-learning-based android malware detection." IEEE Transactions on Industrial Informatics 14.7 (2018): 3216-3225.

[4] Kim, TaeGuen, et al. "A multimodal deep learning method for android malware detection using various features." IEEE Transactions on Information Forensics and Security 14.3 (2018): 773-788.

[5] Bovenzi, Giampaolo, et al. "A comparison of machine and deep learning models for detection and classification of android malware traffic." 2022 IEEE Symposium on Computers and Communications (ISCC). IEEE, 2022.

[6] Gohari, Mahshid, Sattar Hashemi, and Lida Abdi. "Android malware detection and classification based on network traffic using deep learning." 2021 7th International Conference on Web Research (ICWR). IEEE, 2021.

[7] Arora, Anshul, and Sateesh K. Peddoju. "Minimizing network traffic features for android mobile malware detection." Proceedings of the 18th International Conference on Distributed Computing and Networking. 2017

[8] Sihag, Vikas, et al. "De-LADY: Deep learning based Android malware detection using Dynamic features." J. Internet Serv. Inf. Secur. 11.2 (2021): 34-45.

[9] Arora, Anshul, and Sateesh K. Peddoju. "NTPDroid: a hybrid android malware detector using network traffic and system permissions." 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2018.

[10] Hadiprakoso, Raden Budiarto, Herman Kabetta, and I. Komang Setia Buana. "Hybrid-based malware analysis for effective and efficiency android malware detection." 2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS). IEEE, 2020.