딥러닝 기반의 악성 노드 탐지 기법 동향

강예준[1], 김원웅[1], 김현지[1], 임세진[1], 서화정[1]
[1]한성대학교 IT융합공학부
etus1211@gmail.com, dnjsdndeee@gmail.com, khj1594012@gmail.com,
hwajeong84@gmail.com

Deep Learning-based Malicious Node Detection Technique Trend

Yea-Jun Kang[1], Won-Woong Kim[1], Hyun-Ji Kim[1], Se-Jin Lim[1], Hwa-Jeong Seo[1]
[1]Dept. of IT Convergence Engineering, Han-Sung University

요 약

최근 몇 년간 블록체인 기술은 빠르게 발전하여 많은 산업에 영향을 끼쳤다. 하지만 동시에 비트코인, 이더리움 등 블록체인 네트워크 내에서 많은 금융 범죄들이 발생하고 있다. 최근에는 이와 같은 비정상적인 활동을 탐지하기 위해 많은 연구가 진행되고 있다. 본 논문에서는 딥러닝을 기반으로 블록체인 네트워크 내의 악성 노드를 탐지하는 기법에 대해 살펴본다. 대부분의 연구가 높은 정확도를 달성하였으며, 악성 노드뿐만 아니라 악성 노드가 수행한 사기 트랜잭션을 탐지하는 연구도 진행되고 있었다.

1. 서론

최근 몇 년간 블록체인 기술은 빠르게 발전하여 많은 산업에 영향을 끼쳤다. 하지만 동시에 비트코인, 이더리움 등 블록체인 네트워크 내에서 많은 금융 범죄들이 발생하고 있다. 따라서 악의적인 행동을 하는 악성 노드를 탐지하는 것은 매우 중요한 문제이다. 최근에는 이와 같은 비정상적인 활동을 탐지하기 위해 많은 연구가 진행되고 있다. 본 논문에서는 딥러닝을 기반으로 악성 노드를 탐지하는 기법에 대해 살펴본다.

2. 관련 연구

2.1 블록체인

블록체인이란 네트워크 내의 참여자들이 peer-to-peer 방식으로 모두 동일한 원장을 공유하는 데이터 분산 처리 기술을 말한다[1]. 블록체인은 중앙 서버가 장부를 관리하는 기존 방식이 아닌, 암호화된 정자 장부를 네트워크 내의 참여자끼리 모두 공유함으로써 탈중앙화를 실현하였다. 따라서 블록체인 네트워크 내에는 제 3자인 중앙 서버가 존재하지 않으며, 데이터를 위조하기 위해서는 중앙 서버를 해킹하는 것이 아닌 과반수의 네트워크 참여자를 해킹해야한다. 이는 사실상 불가능하기 때문에, 데이터를 조작할 수 없어 무결성을 보장한다. 블록체인의 종류는 네트워크에 누구나 참여할 수 있는 퍼블릭 블록체인과 서비스 제공자의 허가를 받아야만 네트워크에 참여할 수 있는 프라이빗 블록체인으로 나뉜다.

3. 연구 동향

본 논문에서는 딥러닝을 기반으로 블록체인 네트워크 내의 악성 노드를 탐지하는 기법에 대해 살펴본다.

[2]에서는 Externally Owned Account(EOA)와 Smart Contract Account(CA) 악성 노드를 탐지하는 기계 학습 모델 두 개 생성하였다. 해당 연구에서는 여러 저장소로부터 악성 노드와 악의적이지 않은 노드를 수집하여, 각 노드가 실행했던 모든 트랜잭션을 추출하였다. 트랜잭션에는 보낸 사람의 주소와 받는 사람의 주소, 타임 스탬프 트랜잭션에 사용된 가스 값이 포함된다. EOA로부터 추출한 트랜잭션으로부터 30개의 특징을 모델을 학습하는 데에 사용하였으며, CA로부터 추출한 트랜잭션으로부터는 18개의 특징을 통해 모델을 학습시켰다. EAO 탐지 모델과 CA 탐지 모델에 대해 성능을 측정한 결과 각각 96,54%, 96.82%의 정확도를 달성하였다.

[3]에서는 머신러닝 알고리즘 중 하나인 XGBoost 분류기를 사용하여 거래 내역을 기반으로 불법 계정 탐지 기법을 제안하였으며, 어떠한 기능이 불법 계정 탐지에 가장 중요한 요소인지에 대해 논의하였다. 학

습을 위해 불법 활동 (다른 계약 주소 모방, 다른 사용자 모방, 피싱, 웹사이트 미러링 등)을 수행하는 계정과 일반 계정에 대한 분류를 수행하였으며, 이를 위해 XGBoost 모델을 사용하였다. 또한, 학습 기법 중 하나인 교차 검증을 사용하여 0.963(±0.006)의 평균 정확도를 달성하였으며, 이러한 결과에 가장 크게 영향을 미치는 3가지 요소는 '첫 거래와 마지막 거래 사이의 시차(분)', '사용 가능한 총 이더 잔고' 및 '계좌로 받은 이더의 최소 가치'임을 알 수 있었다.

[4]에서는 이더리움 블록체인의 악성 노드를 조사하고 의사 결정 트리 (j48), 랜덤 포레스트 및 K-최근접 이웃 (KNN)의 세 가지 기계 학습 알고리즘을 사용하여 높은 정확도, 최소 시간 및 최소 기능을 달성할 수 있는 사기 탐지 모델을 제안하였다. Kaggle에서 제공하는 42개의 특징값 (전송 최소 값, 수신 최소 값, 고유 수신 주소 등의 트랜잭션 관련 정보)을 갖는 데이터셋으로부터 가장 효과적인 특징을 6개만 추출 (상관계수 사용)하여 새로운 데이터셋을 구축하여 사용하였다. 또한, 해당 데이터셋에 대해 "사기"와 "비사기"로 라벨링하였으며, 전체 특징을 사용한 경우 (Full)와 효과적인 특징을 추출 (Selected)한 경우에 대해 모두 실험하였다. 모델의 성능 평가 지표인 F-measure를 측정한 결과, Full에 대해 의사 결정 트리, 랜덤 포레스트, KNN의 경우 각각 98.4%, 98.4%, 98.7%를 달성하였고, Selected 데이터셋에 대해서는 각각 97.5%, 97.6%, 97.4%를 달성하였다. 또한, selected 데이터셋에 대한 시간 측정 결과, Full에 비해 상당한 개선을 보였다. 따라서 제안 기법은 사기 트랜잭션 탐지에 있어 높은 정확도와 적은 특징 사용, 적은 소요 시간을 달성하였다. 그러나 해당 연구는 불법 계정 탐지가 아닌 불법 계정이 수행한 사기 트랜잭션 탐지에 대한 방법을 제시하였다.

4. 결론

최근 블록체인 기술이 발전함에 따라 악의적인 행위를 하는 악성 노드가 증가하였다. 이와 같은 악성 노드를 탐지하고자하는 연구들이 다수 진행되고 있었으며, 대부분의 연구가 높은 정확도를 달성하였다. 또한 EAO 탐지 모델과 CA 탐지 모델을 각각 구현한 연구도 있었다. 블록체인 내에서 발생하는 악의적인 행위를 탐지하고자, 악성 노드뿐만 아니라 악성 노드가 수행한 사기 트랜잭션을 탐지하는 연구도 진행되고 있었다.

앞으로 악성 노드를 탐지하는 기법을 통해 블록체인을 더욱 다양한 분야에 적용할 수 있을 것으로 사료된다.

5. Acknowledgement

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00264, Research on Blockchain Security Technology for IoT Services).

참고문헌

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized Business Review (2008): 21260.

[2] Kumar, Nitesh, et al. "Detecting malicious accounts on the Ethereum blockchain with supervised learning." International Symposium on Cyber Security Cryptography and Machine Learning. Springer, Cham, 2020.

[3] Farrugia, Steven, Joshua Ellul, and George Azzopardi. "Detection of illicit accounts over the Ethereum blockchain." Expert Systems with Applications 150 (2020): 113318.

[4] Ibrahim, Rahmeh Fawaz, Aseel Mohammad Elian, and Mohammed Ababneh. "Illicit account detection in the ethereum blockchain using machine learning." 2021 International Conference on Information Technology (ICIT). IEEE, 2021.