딥러닝 기반 비트코인 관련 서비스에 대한 디도스 공격 탐지

백의준, 이민섭, 심규석, 박지태, 박준상*, 김명섭
고려대학교, LG전자
{pb1069, chenlima2, kusuk007, pjj5846, tmskim}@korea.ac.kr, junsang.park@lge.com*

DDoS Attack Detection in Bitcoin-Related Services based on Deep Learning

Uijun Baek, Min-Seob Lee, Kyu-Seok Shim, Jee-Tae Park, Jun-Sang Park*, Myung-Sup Kim
Korea University, LG Electronics*

요 약

본 논문은 딥러닝을 이용하여 비트코인 관련 서비스에서 발생하는 디도스 공격을 탐지하는 방법을 제안한다. 블록체인 기술이 적용된 첫 암호화폐인 비트코인이 암호화폐 시장을 개척한 이래로 많은 블록체인 기술을 기반한 암호화폐와 서비스들이 개발되고 있다. 이에 암호화폐 뿐만 아니라 서비스의 취약점 및 기술적인 결함을 통해 공격하여 시스템의 존속 여부와 막대한 금전적인 피해를 입히는 사례들이 발생하고 있다. 이러한 공격에 대한 분석 또는 많은 대응책들이 제시되고는 있으나 공격이 발생했을 때 이를 탐지하거나 예방할 수 있는 방법에 대해서는 많은 연구가 이루어지고 있지 않다. 이에 본 논문은 딥러닝을 이용하여 실제 공격 사례와 비트코인 네트워크 데이터를 학습하여 관련 서비스에서 발생하는 디도스 공격을 탐지하는 방법을 제안한다. 본 논문에서는 비트코인 네트워크 데이터 및 실제 사례를 수집하는 방법, 수집된 데이터를 탐지에 적절하게 전처리 하는 과정, 데이터를 학습하고 테스트 후 평가하는 방법에 대해 서술한다.

Ⅰ. 서 론

사토시 나카모토에 의해 블록체인 기술이 적용된 첫 암호화폐인 비트코인이 개발되고 난 후 블록체인 기술을 기반으로 한 많은 암호화폐와 서비스들이 개발되고 있다[1]. 특히, 비트코인은 적절한 대체화폐인가에 대한 의문에도 불구하고 현재까지도 시장규모와 거래규모에서 순위권을 차지하고 있다. 이러한 암호화폐 시장의 성장세에 따라 이를 위협하는 악성 행위들이 발생하고 있으며 이러한 행위들은 블록체인 기술의 취약점 및 간접적으로 관련이 있는 서비스에 대한 공격에 초점이 맞추어져 있다. 현재까지도 많은 공격들이 발생하고 있는 가운데 이를 분석하고자 하는 시도는 많지만 실용적으로 이를 탐지하고 예방하는 것에 대한 연구는 부족한 실정이다. 이에 본 논문에서는 비트코인 네트워크에 발생한 실제 디도스 공격 사례와 비트코인 네트워크의 데이터를 학습하여 디도스 공격을 탐지하는 방법을 제안한다.

본 논문은 서론에 이어 관련연구에서 디도스 공격을 분석했던 연구에 대해 설명하며 본론에서 비트코인 네트워크와 실제 디도스 공격 사례를 수집하는 방법, 수집된 데이터를 탐지에 적절하게 전-처리 하는 방법, 데이터를 학습하고 테스트하는 방법과 실험 결과를 평가하는 방법에 대해 서술한다. 마지막으로 결론에서 제안한 방법에 대한 평가와 한계점에 대해 서술하고 향후연구를 제시하며 마친다.

Ⅱ. 관련 연구

[2]는 2011년부터 2013년까지 비트코인 관련 서비스에서 발생했던 디도스 공격들을 분류하고 분석하였으며 대부분의 디도스 공격들은 마이닝풀과 거래소에서 발생했다고 밝혔다. 또한 디도스 공격 방어 솔루션을 채택하지 않은 서비스가 솔루션을 채택한 서비스 대비 3배 이상 공격을 받았으며 규모가 큰 마이닝풀일수록 더 많은 공격을 받는다고 밝혔다. 실험에 사용했던 디도스 공격 사례들은 하버드 데이터 서버에 저장되어 있다[3]. 본 논문에서는 [2]에서 사용했던 디도스 공격 사례 데이터를 이용하여 디도스 공격 탐지 실험을 수행하여 실험의 객관성을 갖추고자 하였다.

Ⅲ. 본론

본 장에서는 데이터를 수집하고 전-처리 하는 과정과 데이터를 학습하여 테스트하는 과정 마지막으로 평가하는 과정을 서술한다.

A. 데이터 수집

비트코인 네트워크는 비트코인 클라이언트 프로그램의 *getblock* 명령어를 통해 수집하며 블록과 트랜잭션의 데이터를 동시에 수집하기 위해 옵션값을 2로 주어 수집하였다.

비트코인 관련 서비스에서 발생했던 실제 디도스 공격 사례는 [3]에서 다운로드받아 사용하였으며 이는 디도스 공격이 발생한 날짜, 발생했던 서비스의 이름, 서비스의 타입 그리고 공격을 보고했던 보고서의 인덱스를 포함한다. 이로부터 공격이 발생한 날짜에 생성된 블록에는 1로 공격이 발생하지 않은 날짜에 생성된 블록은 0으로 라벨링한다.

B. 통계 데이터 추출

통계 데이터는 수집된 데이터로부터 0~2 단계의 추출과정을 거치며 총 84개의 데이터를 수집하며 이 과정은 표1에서 보인다.

C. 특징 추출

통계 데이터를 추출하는 과정에서 많은 중복과 불필요한 데이터가 추출되었을 것이므로 주성분 분석을 통해 분석 및 탐지에 적절한 데이터를 제거하는 과정을 거친다. 주성분 분석을 통해 원래 데이터가 표현할 수 있는 차원의 99%까지 표현하는 데이터를 추출한다. 특징 추출을 통해 학습에 사용하는 특징의 개수를 84개에서 22개까지 감소시켰으며

이 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업이며 (NRF-2018R1D1A1B07045742) 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2018-0-00539-002,블록체인의 트랜잭션 모니터링 및 분석 기술개발)

데이터의 크기도 대략 1/4 정도 줄일 수 있었다.

Data Level	Raw data (0^{th})	1st Extraction	2nd Extraction	Number of data
Block	nTx			1
	Weight			1
	Size			1
	vSize			1
Transaction	nVin		Sum Max Min Avg Stdv (5)	5
	nVout			5
	Value			5
	Fee			5
	Tx_vSize			5
	Tx_Size			5
Input & Output of Transaction	Vout_value	Sum Max Min Avg Stdv (5)		25
	Vin_value			25

표 1 수집된 데이터의 통계 처리 과정 및 결과

D. 학습 및 테스트 과정

본 논문에서는 적절한 실험을 위해 전체 데이터 셋을 6 : 2 : 2 의 비율로 학습 셋, 검증 셋, 테스트 셋으로 나누었으며 학습을 위해 다층 퍼셉트론 모델을 사용하였다. 학습을 위해 설정한 하이퍼 파라미터는 표2에 나타나 있다. 우리는 다양한 실험을 위해 학습 횟수와 레이어의 개수를 변경시켜가며 실험하였다.

Parameter	Value	Parameter	Value
Learning Rate	0.01	#Nodes of hidden layer	84
#Epochs	10000 ~ 500000	#Hidden Layers	3 ~ 12

표 2 학습을 위해 설정한 하이퍼 파라미터

Ⅳ. 본론

본 장에서는 실험 결과를 평가하고 결과에 대해 서술한다. 탐지 결과는 설정한 다양한 하이퍼 파라미터에 따라 3차원 그래프로 보여지며 우리는 그래프를 보며 탐지에 적절한 하이퍼 파라미터로 설정된 모델을 찾는다. 탐지에 있어 정확도는 공격이 발생한 날짜에 생성된 모든 블록 중 일정 임계치 이상의 블록 데이터가 탐지 되었을 때 해당 디도스 공격이 탐지되었다고 판단하며 반대로 공격이 발생하지 않은 날짜에 생성된 모든 블록 중 일정 임계치 이상의 공격 블록데이터가 탐지되지 않았을 경우 해당 날짜는 디도스 공격이 발생하지 않았다고 판단한다. 본 실험에서는 다양한 실험결과에 따라 도출된 최적의 임계치를 설정하고 평가하였다.

A. 학습 결과

학습 결과는 그림 1과 같으며 많은 은닉층의 개수일수록 정확도가 높아지는 것을 확인할 수 있었으며 학습 횟수보다는 은닉층의 개수가 정확도에 영향을 많이 미치는 것을 확인하였다. 또한 디도스 공격이 발생한 날짜와 발생하지 않았을 날짜를 적절하게 구분하는 것을 확인하였다.

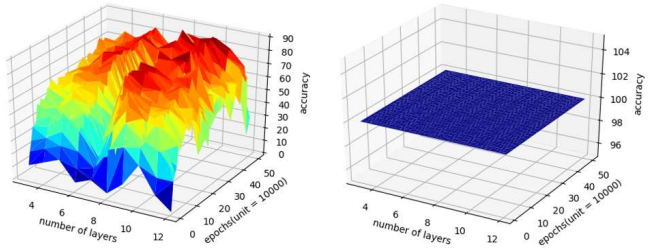

그림 1 디도스 공격이 발생한 날짜(좌)와 발생하지 않은 날짜 학습 결과(우)

B. 검증 결과

검증 결과는 그림 2와 같으며 특히 은닉층의 개수가 9개 일 때 높은 탐지정확도를 보이는 것을 확인하였다.

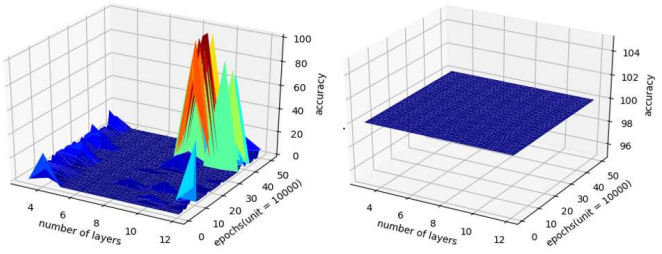

그림 2 디도스 공격이 발생한 날짜(좌)와 발생하지 않은 날짜 검증 결과(우)

C. 테스트 결과

테스트 결과는 그림 3과 같으며 특히 은닉층의 개수가 12개일 때 높은 탐지 정확도를 보이는 것을 확인하였다.

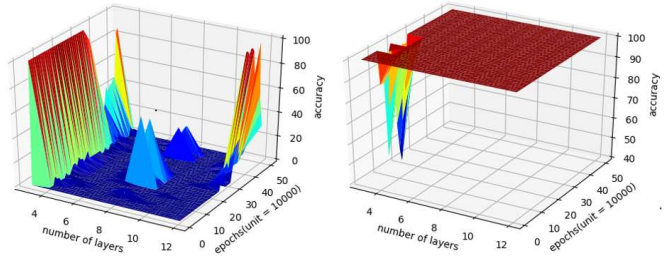

그림 3 디도스 공격이 발생한 날짜(좌)와 발생하지 않은 날짜 테스트 결과(우)

Ⅲ. 결론

본 논문에서는 비트코인 네트워크의 데이터와 실제 사례를 이용한 딥러닝 기반 비트코인 관련 서비스 디도스 공격을 탐지하는 방법을 제안하였다. 우리는 객관성을 갖춘 실험 데이터를 사용하였고 다양한 하이퍼 파라미터 설정에 따른 실험결과의 직관성을 위해 그래프로 나타내었다. 그러나 검증 과정에서 도출한 모델이 테스트 결과 셋에서는 좋지 않은 정확도를 나타내는 한계점을 발견했으며 이에 대해 분석을 수행하였다. 데이터 셋 분석을 수행한 결과, 우리는 검증 셋과 테스트 셋에 포함되어있는 데이터 셋이 동시에 학습될 수 없는 상호배제적인 특성을 지닌 데이터 타입으로 구성되어 있다고 판단하였다. 따라서 각각의 데이터 타입에 대한 다중 모델을 생성하여 탐지를 수행한다면 높은 정확도를 보장할 수 있다. 우리는 상호배제적인 데이터타입을 모두 수용할 수 있는 단일 모델을 구성하고 실용적으로 사용할 수 있는 단일 모델 및 추가 데이터셋 추출에 대해 향후 연구를 진행한다.

참 고 문 헌

[1] NAKAMOTO, Satoshi, et al. Bitcoin: A peer-to-peer electronic cash system. 2008.

[2] Vasek, Marie; Thornton, Micah; Moore, Tyler, 2014, "Replication data for: Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem", https://doi.org/10.7910/DVN/25541, Harvard Dataverse, V2

[3] VASEK, Marie; THORNTON, Micah; MOORE, Tyler. Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. In: International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, 2014. p. 57-71.