비트코인 에코 시스템에 대한 디도스 공격 실시간 탐지 시스템

백의준, 지세현, 신무곤, 심규석, 김명섭
고려대학교
{pb1069, sxzer, tm0309, kusuk007, tmskim}@korea.ac.kr

System Design for Detecting DDoS Attack to Bitcoin Eco-System

Uijun Baek, Se-Hyun Ji, Mu-Gon Shin, Kyu-Seok Shim, Myung-Sup Kim
Korea University

요 약

본 논문은 비트코인 에코 시스템에 대한 디도스 공격을 탐지하는 시스템을 제안한다. 블록체인 기반 암호화폐인 비트코인이 암호화폐 시장을 개척한 이래로 많은 블록체인 기반 암호화폐 및 서비스들이 개발되었다. 이에 암호화폐 및 서비스의 취약점 및 기술적인 결함을 통하여 많은 수의 공격들이 발생하고 있으며 이는 대부분 디도스 공격으로 구성된다. 블록체인 네트워크는 일종의 분산 데이터베이스로서 디도스 공격에 강하며 무결성을 보장한다. 이러한 이유로 블록체인 기반 서비스들이 개발되고 있으나 블록체인 관련 서비스에 발생하는 디도스 공격은 블록체인 네트워크에 간접적인 영향을 줄 수 있으며 이에 관한 연구도 진행되었다. 이러한 공격에 대한 분석 또는 대응책들이 제시되었으나 공격이 발생했을 때 이를 탐지하거나 예방할 수 있는 방법에 대해서는 연구가 이루어지지 않았다. 이에 본 논문은 딥러닝 기반 블록체인 관련 서비스에 대한 디도스 공격을 탐지하는 시스템을 제안한다.

Ⅰ. 서 론

블록체인 기반 암호화폐인 비트코인이 개발된 이래로 많은 블록체인 기반 암호화폐 및 서비스들이 개발되었으며, 특히 1세대 암호화폐인 비트코인과 2세대 암호화폐인 이더리움의 경우 시장규모와 거래량에서 순위권을 차지하고 있다. 이에 암호화폐를 이용한 서비스들이 개발되고 있으며 이러한 암호화폐 시장의 성장세에 따라 이를 위협하는 공격들이 발생하고 있으며 공격 유형의 대부분은 디도스 공격이다. 이러한 공격들은 블록체인 네트워크가 디도스 공격에 강하며 무결성을 보장함을 이유로 네트워크에 대한 직접적 공격이 아닌 관련 서비스 및 응용에 대한 간접적인 공격을 수행한다. 공격이 수행됨에 따라 네트워크에 영향을 미칠 수 있으며 장기적으로 네트워크에 악영향을 줄 수 있다는 연구가 조사되었다. 현재까지도 지속적으로 공격들이 발생하고 있는 가운데 이를 분석하는 시도는 많지만 탐지하고 예방하는 것에 대한 연구는 부족한 실정이다. 이에 본 논문에서는 비트코인 네트워크 관련 서비스에 발생하는 디도스 공격을 딥러닝 기반으로 탐지하는 방법 및 시스템을 제안한다.

본 논문은 서론에 이어 관련 연구에서 디도스 공격을 분석한 연구에 대해 설명하고 본론에서 비트코인 관련 서비스에 대한 디도스 공격 탐지 시스템에 대한 개요 및 세부 모듈에 대해 설명하고 이를 평가하는 방법에 대해 설명한다.. 마지막으로 결론에서 제안한 시스템에 대한 평가와 한계점에 대해 설명하고 향후 연구를 제시하며 마친다.

Ⅱ. 관련 연구

본 장에서는 비트코인 관련 서비스에 발생한 디도스 공격 분석에 대해 수행된 연구를 설명한다.

[1]은 2011년부터 2013년까지 비트코인 관련 서비스에서 발생햇던 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. 마지막으로 이러한 공격들은 장기적으로 비트코인 네트워크에 악영향을 미칠 수 있음을 시사하였다.

본 논문에서는 [1]에서 사용했던 디도스 공격 사례 데이터 [2]을 이용하여 디도스 공격 탐지 시스템을 설계하고 구현하였다.

Ⅲ. 본론

본 장에서는 비트코인 관련 서비스에 대한 디도스 공격 탐지 시스템에 대한 개요와 이를 구성하는 세부 모듈 및 동작 과정을 설명하고 이를 평가한다.

A. 시스템 개요

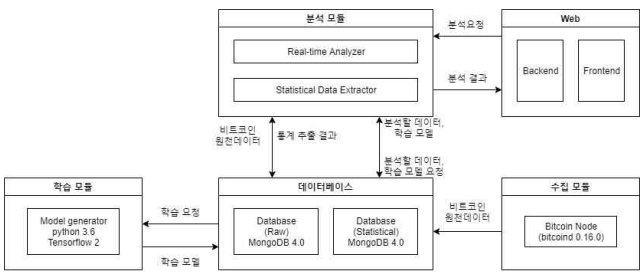

그림 1 실시간 공격 탐지 시스템 개요

그림 1은 실시간 공격 탐지 시스템에 대한 간단한 구조를 나타낸다. 시스템은 크게 수집 모듈, 데이터베이스, 분석 모듈, 학습 모듈 그리고 사용자 요청을 처리할 웹으로 구성되어 있다. 각각의 모듈들은 배포가 용이하도록 도커 컨테이너로 구성되어 있으며 각각의 컨테이너들은 도커 네트워크를 통해 사설망 통신을 한다.

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.2018-0-00539-003.블록체인의 트랜잭션 모니터링 및 분석 기술 개발)

B. 데이터 수집 및 전처리

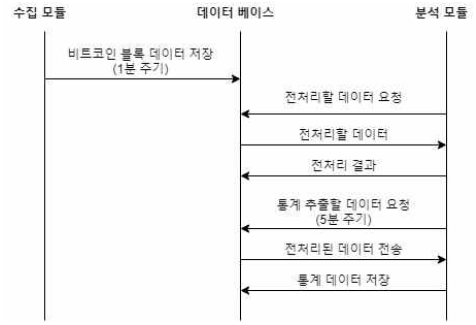

그림 2 데이터 수집 및 전-처리 과정

데이터 수집은 그림 2와 같은 과정으로 이루어진다. 비트코인 네트워크 내 블록이 평균 10분 주기로 생성되나 일정하지 않기 때문에 1분마다 주기적으로 블록 생성 여부를 검사하고 새로운 블록이 생성되었을 때 데이터베이스에 저장한다. 전-처리 과정은 트랜잭션들을 포함하고 있는 전체 블록 데이터로부터 트랜잭션을 분리하여 저장하고 분석에 불필요한 데이터를 제거한다. 전-처리 과정을 거친 데이터는 3개의 레벨로 구분할 수 있으며 블록 레벨, 트랜잭션 레벨, 입·출력 레벨로 구성되어 있다. 추출하는 통계는 총합, 최댓값, 최솟값, 평균 그리고 표준편차로 구성되어 있으며 각 레벨의 데이터는 0~2번의 추출과정을 거친다. 통계 데이터 추출 과정, 목록 및 개수는 그림 3에 나타내었다.

데이터레벨	원천데이터 (0th)	1차 추출	2차 추출	데이터 개수
블록	nTx			1
	Weight			1
	Size			1
	vSize			1
트랜잭션	nVin		총합 최댓값 최솟값 평균 표준편차	5
	nVout			5
	Value			5
	Fee			5
	vSize			5
	Size			5
입·출력	Vout_value	총합 최댓값 최솟값 평균 표준편차		25
	Vin_value			25

표 1 데이터 레벨에 따른 추출된 통계데이터 목록

C. 학습 및 실시간 분석

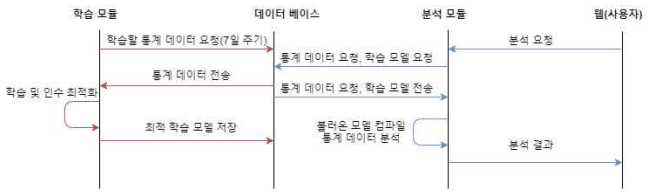

그림 3 학습 및 실시간 분석 과정

학습 과정에서는 실제 공격 사례를 기반으로 라벨링한 84개의 통계 데이터를 학습하여 모델을 생성한다. 딥러닝 모델로는 다층 퍼셉트론을 사용하였고 탐지 성능의 최적화를 위해 3~12 범위의 은닉층 개수 및 10000~500000 범위의 학습 횟수를 학습 인자로 설정하고 검증 정확도가 최고가 되는 모델을 생성한다. 학습 주기는 학습 및 최적화하는데 3일 정도 소요되는 점을 고려하여 일주일로 설정하였다.

실시간 분석과정은 웹을 통해 사용자가 특정 블록 높이의 통계 데이터를 분석 요청하는 것으로 시작한다. 요청을 받은 분석 모듈은 해당 블록 높이의 통계 데이터 및 학습 모델을 데이터베이스로부터 불러와 분석을 수행하고 사용자에게 분석 결과를 제공한다. 실시간성을 갖추기 위해 분석 시스템과 사용자는 웹 소켓 통신을 수행한다.

Ⅳ. 평가

본 장에서는 제안하는 시스템의 탐지 정확도 및 실시간성을 평가한다. 표 2는 탐지 정확도를 나타내며 최적화된 은닉층의 개수와 학습 횟수, 검증 정확도, 테스트 정확도로 구성되어 있다.

은닉층 개수	학습 횟수	검증 정확도	테스트정확도
12	286700	76.72%	68.79%
12	470700	68.15%	67.16%
12	470800	68.15%	67.16%

표 2 제안하는 시스템의 디도스 공격 탐지 정확도

표 3은 제안하는 시스템의 실시간성의 평가결과이다. 본 연구진은 사용자 요청 시 평균 10ms 이내에 분석 결과를 제공하는 것으로 기준을 설정하였으며 객관성 있는 평가를 위해 공인인증기관을 통해 시험을 수행하였다. 시험과정에서 분석 모듈은 무작위로 선택된 10000개의 블록을 10회 분석하고 사용자에게 결과를 전송하여 총 10만 번의 분석을 수행하였다.

시험 항목	시험 목표	결과	비고
블록체인 분석서버 질의응답시간	블록 통계 데이터 분석 요청시, 평균 10ms 이내에 결과 전송 여부	평균 : 8.868ms	최댓값: 369.939ms 최솟값 : 0.135 ms

표 3 제안한 시스템의 실시간성 평가 결과

Ⅴ. 결론

본 논문에서는 비트코인 관련 서비스에 대한 디도스 공격 탐지 시스템을 제안하였으며 설계한 시스템을 실제 구현하고 공격 탐지 시스템의 탐지 성능과 실시간성을 평가하였다. 객관적인 평가를 위해 공인인증기관을 통해 시험을 수행하였으며 이를 통해 제안하는 시스템이 사용자에게 실시간으로 분석 결과를 제공할 수 있음을 나타내었다. 그러나 제안한 시스템이 높지 않은 탐지 성능을 보이며 이는 학습에 사용한 다층 퍼셉트론 모델이 단순하다는 점과 추출되는 통계데이터가 적기 때문이라고 예상된다. 따라서 본 연구진은 지속적인 딥러닝 모델 개발 동향 모니터링을 통해 탐지 모델을 고도화하고 왜도, 첨도, IQR 등 추가 통계추출을 통해 시스템의 탐지 성능을 높일 계획이다.

참 고 문 헌

[1] 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.

[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