블록체인 기반 모바일 리워드 응용의 부정 리워드 획득 탐지 연구

김기현°[1], 노요셉[1], 박종형[2], 김은실[3], 김영재[1]
[1]서강대학교 컴퓨터공학과, [2]서강대학교 메타버스전문대학원, [3]리얼블록스
{kion777, josephro12, azus, youkim}@sogang.ac.kr, lucy@realblox.kr

Detecting Fraudulent Reward Acquisition in Blockchain-based Reward Applications

Kihyun Kim[1], Joseph Ro[1], JongHyung Park[2], Eunsil Kim[3], Youngjae Kim[1]
[1]Dept. of Computer Science and Engineering, Sogang University
[1]Graduate School of Metaverse, Sogang University, [3]realblox, Inc.

요 약

최근 리워드 응용과 블록체인 기술의 결합으로 인해 암호화폐나 NFT를 사용한 리워드 응용이 새롭게 등장하고 있다. 금전적인 보상을 제공하는 리워드 응용들은 비정상적인 사용자가 악의적으로 리워드를 획득하는 부정 리워드 획득 문제가 발생한다. 따라서, 본 연구에서는 비정상적인 사용자가 부정한 방식으로 리워드를 획득하는 행위를 탐지하여 부정행위를 차단하는 비정상 사용자 탐지 기법을 연구한다. 이를 위해, 본 논문에서는 리워드 응용 환경에서 사용자 기기의 GPS 위치 정보와 리워드 획득량을 기준으로 비지도학습의 일종인 클러스터링 알고리즘을 이용하여 사용자를 위험군과 비위험군으로 분류하고 비정상 사용자를 탐지하는 기법을 제안한다. 더 나아가, 클러스터링 알고리즘만을 사용하여 비정상 사용자를 탐지할 경우 거짓양성(false positive)가 생길 수 있음을 지적하고, Jaccard Index를 사용하여 사용자 간 유사도를 분석해 비정상 사용자 탐지의 정확도를 높이는 기법을 제안한다. 이러한 기법은 단순 클러스터링 알고리즘만 적용한 방식에 비해 거짓양성을 약 52% 줄인다.

1 서론

리워드 응용은 사용자가 광고를 시청하는 등의 주어진 미션을 수행하면 리워드/보상으로 현금, 포인트, 캐시백과 같은 금전적 보상을 주는 모바일 응용을 말한다. 최근에는 리워드 응용에 블록체인 기술을 결합하여 코인과 같은 금전적인 리워드를 제공하는 리워드 응용이 출시되었다 [1].

리워드 응용은 사용자에게 보상의 댓가로 금전적인 보상 또는 코인과 같은 암호화폐를 지급하기 때문에 악의적인 사용자들이 악의적인 방법으로 리워드를 부정 획득하여 재화를 쌓을 수 있는 부정 수급 문제가 있다 [2]. 예를 들어 사용자의 다중 계정 생성을 허용하는 DimeTime [3]과 같은 리워드 응용은 사용자가 타이머를 설정한 시간 동안 다른 응용을 사용하지 않으면 리워드를 지급한다. 따라서 악의적인 사용자는 다수의 모바일 기기에 응용을 구동하여 다량의 보상을 획득할 수 있다. 이러한 문제를 방지하기 위해 본 연구는 사용자의 기기 사용에 대한 행동 패턴 분석을 통하여 부정 행위를 감지하고 차단하는 비정상 사용자 탐지 기법 제안을 목표로 한다. 하지만, 리워드 응용 환경에 맞는 정상적인 사용자와 악의적인 사용자에 대한 분류 기준이 명확하지 않고, 비정상 사용자 탐지를 위해 사용자의 특성 데이터 중 어떠한 정보를 활용해야 하는지 명확하지 않았다.

따라서, 본 연구에서는 악의적인 사용자가 다수의 모바일 기기를 사용하여 리워드를 부정수급하는 상황에서, 사용자 기기의 GPS 위치 정보와 리워드 획득량을 사용한 비정상 사용자 탐지 기법을 제안한다. 이를 위해 비지도 학습의 대표적인 기법인 K-Means 클러스터링을 사용하여 사용자를 위험군과 비 위험군으로 분류하고 위험군으로 분류된 사용자들의 기기의 절대적 위치의 유사도를 통계적 기법인 Jaccard Index를 사용하여 비교하고 이를 기반으로 비정상 사용자를 탐지한다.

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 메타버스 융합대학원의 연구 결과로 수행되었음"(IITP-2023-RS-2022-00156318)"

2 배경지식

비정상 행동 패턴 감지 기술: 비정상 행동 패턴 감지 기술은 크게 지도학습과 비지도 학습을 사용한다. 지도학습은 정답이 레이블링(labeling)된 학습 데이터를 활용해 기계를 학습시켜 주어진 입력 데이터에 대하여 올바른 정답을 맞추게 하는 학습방법이다. 그러나 비정상 행동 패턴 탐지를 위해 지도학습을 사용할 경우 다음과 같은 한계점을 갖는다 [4]. 첫째, 학습 데이터 생성의 문제이다. 사용자의 행동을 학습하기 위해서 필요한 데이터 수집과 라벨링에 상당한 시간이 필요하다. 둘째, 오버 피팅의 문제이다. 이상행동으로 규정한 데이터에 대한 학습이 이루어져 개발자가 설정한 데이터 셋에 학습이 제한된다는 문제가 발생한다. 셋째, 사용자 행동의 일반화의 문제이다. 사용자 개개인의 특성이 다르듯 특정 행동을 비정상 행동으로 규정할 수 없다는 문제가 있다.

반면, 비지도 학습은 레이블링 없는 데이터에 대해 학습할 수 있고, 실시간으로 수집되는 데이터를 학습하여 데이터에 내재된 특성을 다각도로 분석할 수 있는 장점이 있다. 따라서 본 연구에서는 비지도 학습의 일종인 클러스터링 알고리즘을 사용해 비정상 사용자를 탐지한다.

클러스터링 알고리즘: K-Means 클러스터링은 비지도 학습의 대표적인 알고리즘으로 본 연구에서는 비정상 사용자 탐지를 위해 사용이 된다. K-Means 클러스터링 알고리즘의 동작은 다음과 같다.

1. 사용자는 초기에 그룹 개수(k)와 각 그룹의 중심점(Centeroid)를 설정한다. 각 중심점은 그룹의 데이터 구성을 결정하며 이는 사용자가 특정한 값을 지정하여 설정할 수 있다.
2. 개별 데이터는 자기 자신과 각 그룹의 중심점과의 거리를 계산하여 가장 가까운 중심점을 갖는 그룹으로 분류가 된다.
3. 각 그룹에 할당된 데이터들의 응집도를 높히기 위해 그룹의 중심점을 그에 속한 데이터들의 무게 중심값으로 재설정한다.
4. 그룹의 구성이 더이상 변하지 않을 때까지 단계 2와 3을 반복적으로 수행한다.

3 GPS 위치 기반 비정상 행동 패턴 감지

모바일 응용 구조는 클라이언트/모바일 기기와 서버 구조이다. 모바일 기기 사용자들은 각자의 기기에서 리워드 응용을 구동한다. 그리고 사용자는 응용에서 요구하는 미션을 수행하고 미션 성공 여부에 따라서 보상으로 리워드를 획득한다. 하지만, 악의적인 사용자는 재화를 쌓으려는 목적으로 리워드 획득만을 위해 다수의 중고 스마트폰 또는 불법적으로 획득한 모바일 기기들에 리워드 응용을 구동한다. 우리는 이처럼 악의적으로 리워드 응용의 사용을 악용하는 사용자를 *비정상 사용자* 라고 정의한다.

3.1 비정상 사용자 패턴 및 위험군 분류

DimeTime [3]은 블록체인과 리워드 응용을 결합한 대표적인 리워드 응용으로 사용자는 응용의 구동시간에 비례하여 리워드/코인을 획득한다. 비정상 사용자는 DimeTime 응용을 여러 개의 기기들에 설치를 하고, 앞에서 소개한 대로 아래와 같은 패턴으로 불법적으로 리워드를 획득하여 재화를 늘릴 수 있다.

- **(비정상 행동 패턴1)** 비정상 사용자는 수백/수천 개의 모바일 기기들을 공장과 같은 한 장소에서 위치하고, 각 기기에 리워드 응용을 복제하여 구동할 수 있다.
- **(비정상 행동 패턴2)** 비정상 사용자는 차량과 같은 이동 수단으로 모든 기기들을 함께 이동하여 한 장소에서 군집하여 위치하여 쉽게 비정상 사용자로 분류되는 것을 피할 수 있다.

위와 같은 비정상 사용자의 종류를 고려하여 우리는 사용자의 이동량과 리워드 획득량에 따라서 기간 내의 사용자들을 표 3.1과 같이 세 가지 그룹으로 분류한다. 기간 내에 획득한 리워드가 많은 경우 위험군(그룹 A, B)으로 분류하며, 그렇지 않은 경우 비위험군(그룹 C)으로 분류한다. 비정상 사용자는 매우 높은 확률로 위험군(그룹 A, B)에 포함된다.

3.2 비정상 사용자 탐지 알고리즘

본 연구에서는 사용자의 비정상 행동 패턴 감지를 위해 사용자 위치 기반 비지도 학습 방법을 채택한다. 이를 위해 각 모바일 디바이스의 응용의 실행 시간 동안 (i) 사용자의 이동량, (ii) 획득한 리워드 양을 각각 클라이언트/모바일 기기와 서버에서 수집한다. 이후 K-Means 클러스터링을 이용하여 사용자를 표 3.1에 있는 그룹으로 분류하여 비정상 사용자를 탐지한다.

그림 1은 리워드 응용의 구동과 비정상 사용자 탐지를 위한 시스템/소프트웨어 구조 및 동작을 묘사한다. 각 기기는 GPS 수집 모듈을 구동하며 사용자의 위치 정보를 수집한다. 서버는 MariaDB를 구동하며 사용자의 위치 정보와 사용자가 획득한 리워드 정보를 저장/관리한다. 그리고, 비정상 사용자 분석 탐지기는 서버의 데이터 베이스를 사용하여 비정상 사용자를 판별한다.

표 1: 사용자 그룹 및 위험도 분류

그룹	위험도	설명
A	위험군	응용 사용중 이동량이 많고 리워드 획득량이 높은 사용자군
B	위험군	응용 사용중 이동량이 적고 리워드 획득량이 높은 사용자군
C	비위험군	응용 사용중 이동량에 상관없이 리워드 획득량이 높지 않은/보통인 사용자군

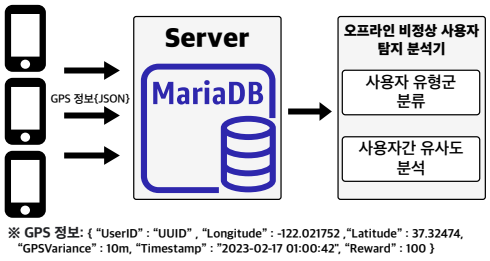


그림 1: 리워드 응용의 시스템 구조와 비정상 사용자 탐지 과정

3.2.1 모바일 기기의 GPS 수집 모듈

GPS 데이터 수집 모듈은 각 모바일 기기에서 구동된다. 응용의 시작과 종료 기간 동안 Δt 시간 간격으로 GPS 위치정보 (기기/디바이스의 위도, 경도, 시간)를 고정된 크기의 디바이스의 로컬 버퍼에 저장한다. 버퍼가 가득 차면/특정 시간에 도달하면 메모리 버퍼에 누적된 GPS 정보를 서버로 전송하여 데이터베이스에 저장한다.

3.2.2 서버의 비정상 사용자 탐지 모듈

서버의 데이터베이스는 사용자의 GPS 정보와 시간에 따른 리워드를 사용자 계정별로 데이터베이스에 저장/관리를 한다. 비정상 사용자 탐지 모듈은 (단계1) 데이터베이스에 저장된 사용자의 GPS와 획득한 리워드 양을 기반으로 사용자 분류하는 단계와 (단계2) 분류된 사용자들 중 실제 비정상 사용자를 탐지 단계를 순차적으로 실행하여 비정상 사용자를 식별한다.

(단계1) 사용자 유형 군 분류: 사용자 유형 군 분류 알고리즘은 다음과 같이 동작한다.

1. 분석 대상 날짜/기간을 입력으로 받고, 데이터베이스에 저장된 해당 기간의 각 사용자별 리워드 양과 이동량(GPS 변화량)을 시각화한다.
2. 서버관리자(비정상 사용자 탐지 책임자)는 그룹 개수 (K)를 3으로 설정한다 (표 3.1과 같이 사용자 유형을 세 가지 그룹으로 분류하는 경우).
3. 서버관리자는 시각화된 데이터의 분포도를 확인하고 각 그룹에 대한 초기 중심점 (T_{GPS}, T_{Reward})를 설정한다.
4. K-Means 클러스터링을 사용하여 표 3.1과 같이 사용자군을 위험군 (그룹 A, B)과 비위험군 (그룹 C)으로 분류한다.

(단계2) 사용자 간 유사도 분석: 단계 1은 사용자의 이동량과 리워드 획득량을 기준으로 사용자의 위험도를 각각 위험군(그룹 A, B)과 비 위험군(그룹 C)으로 분류한다. 하지만 섹션 **??**에서 언급했듯이, 클러스터링 기법은 일반화의 문제가 있어 사용자의 이동량과는 상관없이 정상적인 사용자도 획득량이 많을 경우 위험군 (A, B)으로 분류될 수 있는 거짓 양성(false positive)의 문제가 있다.

한편, 우리는 섹션 3.1에서 비정상 사용자의 패턴 1과 2를 정의했다. 이 패턴들의 공통점은 비정상 사용자들/기기들이 혼자가 아닌, 여러 사용자들/기기들과 클러스터링되어 동일/비슷한 위치의 움직임을 보인다는 것이다. 이러한 특성을 기반으로 위험군 (A, B)로 분류된 사용자들 중에서 실제 비정상 사용자를 가려낸다. 이를 위해 단계 2는 단계 1에서 위험군 (A, B)로 분류된 사용자들/기기들의 절대 위치(GPS의 위도와 경도)의 기록을 기반으로 사용자들 간의 유사도를 판단한다. 유사도 판단으로 Jaccard Index를 사용하여

위치의 변화에 유사도가 높은 사용자들을 분석하고 이들을 비정상 사용자로 판단한다.

Jaccard Index ($JS(A,B) = \frac{|A \cap B|}{|A \cup B|}$)는 Jaccard Similarity Coefficient (계수)로 불리는 대표적인 유사도 분석 인덱스로 두 개의 서로 다른 데이터들 간의 유사도를 구하는 통계적 기법 중 하나이다. Jaccard Index(JI)는 두 집합의 모든 원소에 대하여 교집합을 구하고 그 크기를 두 집합의 크기로 나눈 값으로 정의된다.

4 실험 및 평가

4.1 실험 환경 설정

구현: 사용자 기기에서 구동하는 응용의 위치 정보를 수집하기 위해 iOS 기기를 사용하며 Swift의 CLLocation API를 사용하여 GPS 정보를 그림 1에 있는 형식으로 HTTP 프로토콜을 사용하여 서버에 전송한다. 서버는 MariaDB 데이터베이스를 구동하고, 각 클라이언트로부터 수집한 GPS 위치 정보 및 리워드 획득량을 저장/관리한다. 이러한 정보들을 데이터베이스에 JSON 형식으로 저장된다. 오프라인 분석기는 Python으로 작성되었으며, 데이터베이스에 저장된 사용자별 데이터를 읽어서 앞에서 설명한 비정상 사용자 탐지 알고리즘을 적용하여 비정상 사용자를 탐지한다.

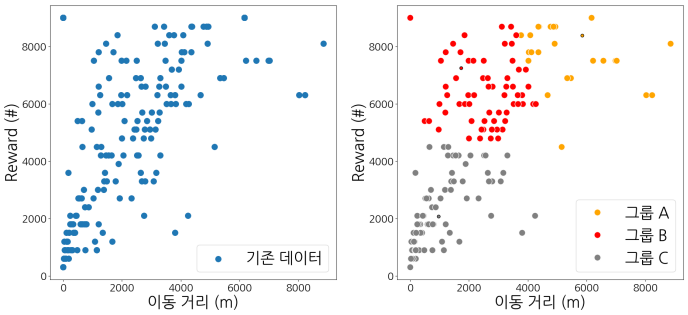
워크로드: 모바일 리워드 응용 환경에서의 실제 사용자 위치 정보에 관한 데이터 셋이 없기 때문에 공공 데이터로 제공되어 있는 Microsoft의 Geolife GPS trajectory dataset [5]을 수정하여 실험에 사용하였다. 해당 GPS 데이터 셋은 아시아에 위치한 182명의 사용자의 2007년 4월부터 2012년 8월까지 이동한 GPS 정보로 구성된다. 실험의 편의를 위해 사용자별 평균 이동량이 0-7km가 되도록 설정하였다. 또한 사용자는 0-9000사이의 리워드를 임의로 부여받고, 리워드 양에 비례하게 GPS 좌표(위도, 경도)의 개수를 가진다. 마지막으로 사용자가 악의적으로 다수의 기기를 사용하여 높은 양의 리워드를 부정수급하는 상황을 설정하기 위해 실험 워크로드/데이터셋에 섹션 3.1에서의 비정상 패턴으로 행동하는 사용자 데이터를 추가하였다. 이들은 총합 60대의 모바일 기기를 사용하여 높은 양의 리워드를 획득한다.

4.2 결과 및 분석

본 연구에서 제안한 비정상 사용자 탐지 알고리즘의 효용성을 분석하기 위해 워크로드 내 사용자의 GPS 정보를 수집한 후 비정상 사용자 탐지 모듈을 적용하여, 모듈의 수행 단계별 결과를 확인 및 검증하였다.

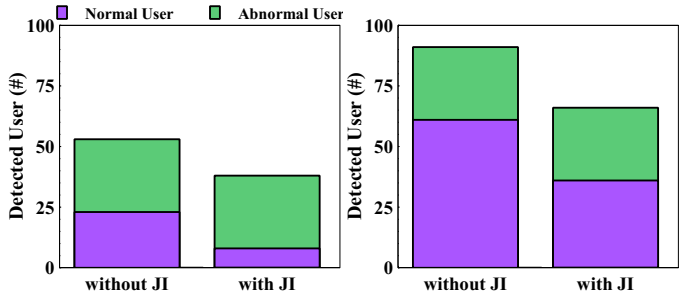
K-Means 클러스터링 결과: 첫번째로 모듈의 수행 **(단계1)**인 사용자 유형 군 분류를 위해(T_{GPS},T_{Reward})을 각각 (4000, 0) (0, 8000) (8000, 8000)으로 설정하여 K-Means 클러스터링을 수행하였다. 그 결과는 그림 2와 같다. 본 연구에서 목표로 하는 분류인 표 3.1과 같이 사용자 그룹이 이동량 및 리워드에 따라 위험군 A, 위험군 B 그리고 비 위험군으로 분류된 것을 확인 할 수 있다.

Jaccard Index 적용의 효과: 본 연구에서 제안하는 탐지 알고리즘의 정확도를 평가하기 위해 JI를 적용하지 않고 단순히 K-Means 클러스터링만 사용한 모듈(without JI)과 JI를 적용한 모듈(with JI)의 거짓 양성 탐지(실제 정상 사용자이나 비정상 사용자로 탐지한 경우) 비율을 측정하였다. 그 결과는 그림 3와 같다. 먼저 두 모듈 모두 위험군 A, B간 거짓양성 탐지 수를 비교했을 때 위험군 A



(a) 클러스터링 이전의 데이터 (b) 클러스터링 결과 (3개의 그룹)

그림 2: 실험 워크로드상의 K-Means 클러스터링 적용 결과



(a) 위험군 A (b) 위험군 B

그림 3: without JI 모듈과 with JI 모듈의 비정상 사용자 탐지 결과

보다 위험군 B에서 거짓양성으로 탐지된 수가 더 많음을 확인 할 수 있다. 이는 위험군 A에 비해 위험군 B의 사용자 이동량이 적어 사용자 간의 이동 패턴이 유사하기 때문이다. 또한 두 위험군 A,B에서 without JI 모듈을 적용하였을 경우 평균적으로 84개의 거짓양성이 발생하였고, with JI를 적용하였을 때 평균적으로 44개의 거짓양성이 발생하였다. 이를 통해 with JI 모듈은 without JI 모듈보다 평균적으로 52%정도 거짓양성 탐지 비율을 줄였음을 알 수 있다. 이는 본 논문에서 제안하는 비정상 탐지 기법이 단순 클러스터링 알고리즘만을 사용한 기법 보다 더 높은 탐지 정확도를 갖는다는 것을 의미한다.

5 결론

본 연구는 블록체인 기반 모바일 리워드 응용에서 악의적으로 리워드를 부정수급하는 사용자 탐지를 목적으로 하였다. 이를 위해 비지도 학습의 대표 알고리즘인 K-Means 클러스터링 및 Jaccard Index 기법을 혼합 사용한 비정상 사용자 탐지 알고리즘을 제안하였다. 그 결과 단순히 K-Means 클러스터링을 사용한 방법 보다 Jaccard Index를 혼합 사용한 방법이 거짓양성 발생률을 약 52% 줄여 탐지 정확도를 높일 수 있었다.

참고 문헌

[1] S. Verma, S. Dash, A. Joshi, and Kavita, "A detailed study of blockchain and dapps," in *2022 International Conference on Cyber Resilience (ICCR)*, pp. 1–5, 2022.

[2] 좌영길, "경찰, '리워드 앱' 계정 1만개로 수천만원 포인트 적립 30대 입건," 2014,11.12. https://www.etoday.co.kr/news/view/1018181.

[3] Realblox, "Don't play to earn - dimetime," 2023. https://www.dimetime.io/en/.

[4] O. A. Baki, J. Zhang, M. Griss, and T. Lin, "A mobile application to detect abnormal patterns of activity," in *Mobile Computing, Applications, and Services* (T. Phan, R. Montanari, and P. Zerfos, eds.), (Berlin, Heidelberg), pp. 190–202, Springer Berlin Heidelberg, 2010.

[5] Y. Zheng, H. Fu, X. Xie, W.-Y. Ma, and Q. Li, *Geolife GPS trajectory dataset - User Guide*, geolife gps trajectories 1.1 ed., July 2011.