정 보 보 호 학 회 지
제 30 권 제5호, 2020. 10

# 온라인게임 분야의 Data-driven Security

김 휘 강*

요 약

온라인게임은 부정로그인 및 게임봇 (Game BOT) 탐지 등 서비스에 악영향을 주는 이상징후를 조기에 탐지해야 하는 서비스 분야이다 보니, 데이터기반 보안 (Data-Driven Security)이 상당히 오랜 기간 자생적으로 구축이 되어왔다. 온라인게임은 초당 동시접속이 800만~1천만에 육박하는 게임도 시장에 빈번히 존재하기 때문에, 게임유저들의 로그데이터를 빅데이터 기술을 접목한 데이터 분석이 필수적이다. 본고에서는 온라인게임 분야에 존재하는 다양한 위협요소 중 하나인 게임봇 및 작업장 탐지에 적용된 데이터기반 보안 기술들에 대해 조사하고 향후 온라인게임분야에서의 데이터기반 보안의 연구 방향을 제시해 보고자 한다.

## Ⅰ. 서 론

데이터기반 보안 (Data-Driven Security) 란 침입이나 이상징후 탐지를 하는데 있어 단순히 규칙기반 (rule-base)나 휴리스틱에 의존하지 않고, 데이터 분석 결과에 입각하여 판정을 하는 정보보안체계를 말한다. 즉, 분석가의 주관적 견해가 의사결정에 개입될 여지를 최소화 하고 객관적인 의사결정이 가능한 장점이 있다. 이러한 특징 때문에, 데이터기반 보안은 오탐을 극히 최소화해야 하는 서비스환경 또는 사람의 안전 (safety)이 극히 요구되는 제품과 관련된 보안분야에 널리 확산되고 있다.

데이터기반 보안이 적용된 예로는 금융분야에서의 이상증후탐지시스템 (Fraud Detection System; FDS), 온라인게임분야에서의 게임봇 탐지시스템 등을 들 수 있다.

이 중, 본고에서는 데이터기반 보안 중 온라인게임보안에 데이터기반 보안이 적용된 연구들을 중심으로 다루어보고자 한다.

온라인게임은 인터넷에서 가장 많은 이용자들이 이용하는 대표적인 응용서비스라 할 수 있다. 예컨대, “리그오브레전드” 게임의 경우에는 2019년 현재 초당 동시접속이 800만명 이상이 될 정도로 대규모의 이용자들이 즐기고 있다. 온라인게임에서는 이용자들이 플레이를 하면서 획득한 경험치, 아이템들에 대한 기록을 실시간으로 기록 및 반영해야 하기 때문에 게임플레이 중 발생한 기록들을 데이터베이스 또는 로그파일의 형태로 저장을 하고 있다. 이렇게 저장된 기록을 이용하여, 시스템 장애로 인해 반영되지 못한 데이터들이 있는지 대조를 하는데 사용하거나, 게임 내 버그를 이용하여 치팅 (cheating) 플레이를 한 이용자를 적발하거나, 게임 내 아이템을 부정한 방법으로 획득하여 부정한 이익을 얻은 불량 이용자들을 탐지하는데 활용하고 있다. 특히, 온라인게임은 다수의 이용자들이 동시에 대규모다중접속 (Massive Multi-Player)을 하며 상호작용을 하기 때문에, 이러한 게임내 부정행위 (예: 치팅 플레이, 게임 내 사기, 게임 내 버그 악용)를 조기에 탐지하여 제재를 하지 않으면 정상적인 플레이를 하는 이용자들의 불만이 발생할 수 있다. 더불어 이러한 제재를 하는 과정에서 잘못된 판단으로 인해 정상적인 이용자를 악성행위를 한 이용자로 오인하여 제재를 할 경우 이용자가 게임을 떠나거나, 게임회사와 분쟁이 발생할 수 있으므로, 무엇보다도 오탐을 발생시키지 않으면서 객관적이고 정확한 판단을 내리는 것이 중요하다. 게임모니터링을 하는 인원에 의해 육안에 의한 관찰이나 수작업에 의한 단편적인 데이터 분석을 할 경우, 일부 하드코어 유저들의 행위들이 치팅플레이와 유사한 것으로 오인받을 수 있는 문제가 발생할 수 있기 때문에, 빅데이터에 의한 대규모 데이터의 분석, 기계학습을 이용한 정확도 높은 탐지모델을 구현하는 것이 반드시 필요하다.

* 고려대학교 정보보호대학원 (교수, cenda@korea.ac.kr)

예를 들어 동시접속자 수 800만명의 게임에서, 게임 유저 1명이 초당 2건의 게임액션 (게임 내 이동, 공격, 주문 등의 게임 내 행위)을 하고, 1건의 게임액션 당 40 바이트 (예: 타임스탬프, 액션 명, 이용자 정보, 맵 정보, 액션 대상체, 아이템 습득 여부 등)의 로그를 남긴다고 가정해 볼 경우, 텍스트 데이터로 약 25.1 테라바이트 만큼의 로그파일이 매일 생성된다. (40bytes/초 x 60초/분 x 60분/시 x 24시 x 8,000,000 = 약 25.1테라바이트)

즉, 온라인게임 서비스에서 데이터분석에 입각한 의사결정은 서비스보안을 위해 반드시 필요하고, 처리해야 할 데이터의 사이즈는 다른 인터넷 서비스에 비해서도 상당히 크기 때문에, 데이터기반 보안 분야 중에서도 도전적인 산업군이라고 볼 수 있다.

## Ⅱ. 온라인게임보안 위협 및 보안기술 분류

### 2.1. 온라인게임 보안의 세대별 분류

온라인게임 보안과 관련된 기술은 크게 다음과 같이 세대를 나누어 볼 수 있다.

1세대는 클라이언트 단에서 역공학 방지 기술을 이용하여 온라인게임 치팅 툴 (매크로, 게임핵, 메모리 변조 프로그램 등)이 게임클라이언트 프로그램을 후킹하여 게임클라이언트에서 게임서버로 전송되는 데이터를 위변조하는 것을 차단하는 기술이다. 이는 데이터기반 보안이 적용되지 않은 가장 고전적인 온라인게임 보안 기술로서, 온라인게임 태동기부터 2000년대 초반까지 주로 활용된 기술이라고 할 수 있다.

2세대는 본격적으로 데이터기반 보안 기술이 적용되기 시작한 시점으로 볼 수 있으며, 2000년대 초반부터 2010년 정도까지 주로 MMORPG (Massively Multiplayer Online Role Playing Game) 장르에 적용되어 왔었다. 이 시기에는 서버단에서 데이터마이닝 기법을 이용하고, Decision Tree, Random Forest, SVM 과 같은 전통적인 분류기 (classifier)를 적용하여 정상 이용자와 비정상 이용자로 분류 (classification)하는 수준이라고 볼 수 있다.

3세대에서는 서버단에서 데이터마이닝을 이용하되, 분석의 정확도를 높이고 분석 부하량을 낮추기 위해 선별적인 외과적 수술 방식으로 부정이용자들을 탐지해 내는 방식으로 진화하였다. 즉, 2세대에서는 모든 이용자들에 대해 분석을 일괄적으로 하여 부정이용자들을 탐지해 냈다면, 3세대에서는 기업화되고 대규모로 게임 내 사이버재화를 수집한 뒤 현금화 하려는 시도를 하는 작업장에 특화된 탐지기법을 개발하는데 집중되어 있다.

3세대 기법들은 PC기반게임들에서 모바일게임으로 온라인게임시장이 재편되기 전까지 2010년부터 2010년대 중반까지 활발히 개발되었으며, 2010년대 후반에는 딥러닝 기술을 적극 반영하여 탐지 정확도를 향상시키는 형태로 진화되었다.

2015년~2020년 까지는 딥러닝을 적용하여 게임 내 부정이용자들을 적발해 내는 방식 또는 다양한 분석 모델 (예: 악성행위 전파 모델)을 수립하고 소셜네트워크 분석기술과 접목시킨 분석기법 등 hybrid 한 기법들이 다양하게 적용되어가고 있어서 이 시기에 개발되고 있는 데이터 분석 기반 온라인게임 보안 기법들을 편의상 4세대로 구분할 수도 있다.

### 2.2. 온라인게임 내 보안 위협

온라인게임 서비스 상에서 데이터기반 보안을 이용하여 탐지를 해야 하는 보안 위협으로는 대표적으로 게임봇, 계정도용, 게임 내 사기 등이 있다. 이 중 가장 위협적인 온라인게임 상의 보안 위협으로는 “게임봇” 이라 불리는 자동 플레이 프로그램이다. 게임봇은 게임 이용자의 직접적인 조작 없이 프로그램을 이용하여 자동으로 게임을 플레이를 하는데, 사람의 경우 이용 시간 제약, 피로로 인하여 최대 플레이 시간에 자연스럽게 한계가 있는 반면, 게임봇을 이용한 플레이의 경우에는 탐지되지 않는한 게임 플레이를 24시간 지속하는 것이 가능하므로, 정상적인 이용자에 비해 게임 내 빠른 성장과 빠른 대규모 게임 내 재화 획득을 할 수 있다. 그렇기 때문에 게임봇 이용자를 적시에 탐지하여 제재를 하지 못한다면, 정상적인 게임 이용자와 게임봇을 이용한 부정이용자들간에 게임 내 부의 격차가 심해져 게임 내 밸런스를 파괴하고 정상적인 게임 이용자가 박탈감을 느껴 이탈하는 등 게임서비스의 지속에도 악영향을 끼치게 된다. 특히, 게임봇을 대규모로 이용하여 전문적으로 게임 내 재화를 부정 취득한 뒤 이를 현금으로 교환하여 부당이익을 취하는 기업화된 집단이 출현하게 되었는데, 이를 “작업장 (Gold-Farming Group; GFG) 라 부른다 [40][42].

데이터기반 보안기법을 적용하여 정상적인 이용자인데 장시간 게임을 즐기는 헤비유저와 게임봇 이용자를 오탐 없이 구분해 내는 것이 중요하며, 대규모로 게임봇 이용자를 제재할 경우 한시적으로 게임 내 아이템의 수요공급 균형이 깨지는 부작용이 발생할 수 있으므로, 기업화된 작업장을 최우선적으로 식별해 내어 외과적 수술 방식 (surgical strike)으로 제재를 하는 것 역시 중요하다고 할 수 있다.

## Ⅲ. 문헌 연구

### 3.1. 온라인게임 보안 기술 분류

Yan은 초기 연구에서 온라인게임에서 부정행위 탐지 및 대응방법에 대해 부정행위 방지를 위해 시스템적인 디자인 설계, 침입 탐지를 위한 네트워크 및 호스트 기반의 IDS 사용, 평판 관리 시스템을 제시하였다 [1].

Woo 등은 온라인게임 내 위협 및 적용할 수 있는 데이터기반 보안 기법들에 대해 적용 위치에 따라 클라이언트단, 네트워크단, 서버단으로 분류를 제시하였다 [2].

1세대와 2~3세대에 해당하는 주요 연구들에 대해 정리하면 [표1]과 같다.

클라이언트는 항상 역공학에 의해 분석당할 우려가 있고, 클라이언트 단에서 분석 및 탐지를 직접 수행할 경우 이용자의 컴퓨터의 리소스를 과도하게 소모하여 게임성을 떨어뜨리는 문제가 있어서, 대부분의 데이터 기반 보안은 서버단에서 플레이 로그 분석을 기반으로 이루어지고 있다.

Mishima 등은 게임 플레이 로그를 분석하여 캐릭터들의 행위별 (예: 전투, 이동, 사냥, 거래 등) 빈도 와 속도를 분석하여 이를 피쳐 (feature) 로 구성하였고, 전통적인 통계기법을 이용하여 게임봇과 일반 사용자를 분류하였다 [3]. Fujita 등은 게임 내 아이템 거래 기록을 네트워크분석을 하고 SVM을 적용하여 현금거래 (Real Money Trade; RMT) 탐지 방법을 제시하였다. Ahmad 등 [5]과 Chen 등 [6]의 연구들에서는 데이터 마이닝 기법과 전통적인 분류기인 Naive Bayes, Bayes Network, Logistic Regression, KNN, J48, AdaBoost 들을 적용하여 게임 내 부정이용자들을 식별하였다.

〔표 1〕 탐지 단별, 적용기술 세대에 따른 분류

| 분류 | 연구 | 특징 |
|---|---|---|
| 서버단 (4세대 중 딥러닝 중심 연구) | [52-55] | 대규모 데이터 분석에 입각한 게임봇 및 작업장 탐지 알고리즘 제시 |
| 서버단 (4세대 중 모델링 중심 연구) | [46-51] | 확산모델을 설계하여 악성행위자의 행위가 타유저들에게 전파되는지를 검증<br>영향력이 큰 악성행위자만 선별적으로 제재하는 모델 제시 |
| 서버 단 (2세대~3세대 연구 위주) | [3-39] | 서버에 저장되는 게임 유저들의 게임 플레이 로그 분석을 통해 수행<br>제재시점 및 제재 규모를 게임회사 정책에 따라 유연하게 통제가능 |
| 클라이언트 단 (1세대 연구 위주) | [43-45] | 클라이언트 단에서 상세한 정보를 수집 가능<br>역공학에 취약하며, 게임의 이용성을 저하시킴 |

### 3.2. 전통적인 분류기를 적용한 데이터기반 보안 예

전통적인 분류기는 상대적으로 오랜 기간 분류 (classification)와 군집화 (clustering)에 사용되어 온 알고리즘들로서, Decision Tree, SVM, Näive Bayes, KNN, Logistic Regression들을 예로 들 수 있다.

이러한 기법들을 적용하는 경우 정확도는 최근 활발히 적용되고 있는 딥러닝 모델들 보다 다소 떨어질 수는 있지만, 해석력이 높으며 학습에 들어가는 시스템 리소스가 상대적으로 적다는 강점이 있다. 그리고 도메인 지식 (domain knowledge)을 활용하여 유의미한 피쳐들을 잘 도출할 경우 딥러닝을 적용하지 않더라도 높은 정확도를 보인다는 점에서 여전히 큰 의미를 갖는다. 게임봇은 프로그램이기 때문에 게임 내 대화의 욕구나 친구들과의 사회화 (socialization) 욕구가 발생하지 않지만, 사람이 플레이하는 경우에는 다양한 유형의 사회화 욕구가 필요하다는 점에 착안한 Kang 등의 연구가 도메인 지식을 잘 활용하여 전통적인 분류기를 사용하였으면서도 높은 정확도를 보여준 연구의 예라 할 수

있다 [12]. 더불어 대용량의 데이터를 복잡한 알고리즘을 사용하지 않고도 치팅툴을 사용한 FPS 게임 플레이어는 다른 사용자들에 비해 승리 비율이나 헤드샷 성공 비율이 플레이 누적시간에 비해 비정상적으로 높을 것이라는 도메인 지식을 활용하여 FPS 에서의 치팅 플레이를 탐지하는 연구를 한 Han 등의 연구 역시 도메인 지식을 잘 활용한 예라 할 수 있다 [13].

[표 2] 는 각 연구들에서 쓰인 피쳐들을 정리해 둔 결과이다.

각 기법별로 온라인게임 보안 분야에 데이터기반 보안을 적용한 예를 [표 3]에 정리하였으며 주요 예는 다음과 같다.

SVM 알고리즘은 데이터가 사상된 공간에서 데이터군을 나누는 최적의 경계평면을 찾아내는 알고리즘이다. Thawonmas 등은 서버 단에서 캐릭터 행위 별 빈도를 피쳐로 추출하고, 이를 SVM 알고리즘에 적용하여 MMORPG에서 게임봇을 분류하였다 [22].

Aurangzeb 등은 서버 단에서 캐릭터들간의 네트워크 기반 데이터를 소셜네트워크 분석 기법을 이용하여 작업장을 탐지하였다. 이를 위해 캐릭터들간의 도움 네트워크, 거래 네트워크 관계데이터를 피쳐로 활용하였으며, Näive Bayes, Bayesian Network, J48, KNN, Logistic Regression, Adaboost 알고리즘에 적용하였다 [17].

Chen 등은 서버 단에서 캐릭터의 이동 패턴을 추적하여 피쳐로 추출하고, KNN, SVM 알고리즘을 적용하여 게임봇을 분류하였다 [23].

Oh 등은 서버 단에서 캐릭터의 행위 및 소셜 네트워크 분석을 수행하였는데, Bayesian Network, J48, KNN, Logistic Regression, Näive Bayes, Adaboost 알고리즘에 적용하여 게임봇을 분류하였다 [18].

〔표 2〕 연구 별 주요 피쳐

| 분류 | 연구 | 특징 |
|---|---|---|
| 캐릭터 행위 | [6],[9-14], [16],[19], [21],[22], [29-31], [33],[35], [37],[38] | 부정행위자의 행동 패턴과 일반 사용자의 행동 패턴이 다르기 때문에 구분이 쉬움<br>정확도 향상을 위해서 필요한 피쳐들이 많기 때문에 많은 자원이 필요 |
| 캐릭터 이동 경로 | [3],[8],[23], [34],[45] | 게임내 캐릭터별, 사용자별 움직이는 경로의 차이가 존재하기 때문에 구분하기 쉬움<br>사용되는 맵에 따라 다르게 적용하는 것이 필요 |
| 소셜 네트워크 데이터 | [4],[5],[7], [15],[17], [18],[24], [26],[27], [28],[36] | 사람들과 함께 하는 온라인게임일 경우 적용이 가능하고 부정행위자와의 구분이 쉬움<br>솔로 플레이를 하는 유저의 경우 부정행위자와의 차이점을 찾기 어려움 |
| 자기 유사도 | [37],[51] | 대규모 MMORPG 에 게임봇의 행위는 자기반복성이 있을 것이라는 특징과 코사인 유사도를 주요 피쳐로 활용 |
| 시퀀스 분석 | [9],[14], [29],[57] | 게임 내 액션을 시퀀스화 하여 바이오인포메트릭 기법을 적용하거나 시퀀스 문자 비교 알고리즘을 활용하여 게임봇을 탐지 |

〔표 3〕 전통적인 분류기를 적용한 연구 분류

| 분류 | 연구 | 특징 |
|---|---|---|
| Decision Tree | [5],[15], [17],[18], [25],[30], [41],[43] | if-then 룰 형태로 해석 가능<br>다른 분류 알고리즘에 비해 낮은 정확도를 가짐<br>빠른 분석 속도가 강점 |
| SVM | [4],[10], [16],[19], [22],[23], [33] | 노이즈 데이터에 영향을 크게 받지 않아 높은 정확도를 가짐<br>분류 결과에 대한 해석이 어려움 |
| Näive Bayes | [8],[9],[17], [18],[29], [30] | 모형이 단순하고 효율적인 계산을 통해 분류 시 높은 정확도를 가짐<br>좋은 결과를 얻기 위해 많은 수의 데이터 필요 |
| KNN | [5],[15], [17],[17], [23],[30] | 학습과정이 빠름<br>모든 데이터에 대한 거리 계산 때문에 데이터 크기가 커짐에 따라 많은 소비 시간을 가짐 |
| Logistic Regression | [5],[17-19], [26],[30] | 계산비용이 적음<br>결과해석을 위한 지식 표현이 쉬움 |
| Bayesian Network | [5],[15], [18],[30], [31] | 변수들 간의 상관관계를 쉽게 이해하는 것이 가능<br>해석력이 높다는 점에서 강점 |
| Adaboost | [5],[15], [18], [30] | 오류율이 낮고, 빠른 연산속도를 가짐 |

## Ⅳ. Research Direction

### 4.1. 빅데이터 분석과 딥러닝 적용의 활성화

최근 몇 년간 글로벌 대규모 온라인게임 회사들을 중심으로, 자체적인 플레이로그 분석용 빅데이터 플랫폼을 구축하였고, 소규모 온라인게임 회사라 하더라도 Google Cloud, Amazon AWS, MS Azure 플랫폼을 이용하여 기성화된 분석 모듈을 이용한 분석이 활성화되고 있어서, 빅데이터 분석기술과 딥러닝 분석기술 장벽은 많이 사라지고 있는 추세이다.

3세대까지의 분석기법의 약점은 대규모 분석을 실시간으로 하기 어려웠기 때문에, 학습에 사용한 데이터셋 수집기간과 탐지에 적용하는 시점의 차이가 발생하면 발생할수록 모델의 변별력이 떨어져 가는 문제가 발생할 수 있다는 점이었다. 더불어 샘플링에 의존한 학습을 하다 보니, 샘플링 기법에 따라 탐지 모델의 성능이 과적합되는 문제점이 있다.

하지만 분석에 활용한 데이터셋의 기간이 길수록, 빠른 주기의 분석이 가능할수록 게임업데이트나 게임봇이용자들의 패턴이 변화함으로 인해 발생되는 컨셉드리프트에 신속히 대응할 수 있게 되며, 이러한 점에서 빅데이터 분석기법을 적용하는 것은 점차 필수적으로 되어갈 것이다.

[9], [52-55] 은 빅데이터 분석 인프라와 장기간의 대용량 데이터를 활용하여 게임봇, 작업장 또는 현금거래를 적발해낸 연구라 할 수 있다.

딥러닝 역시 현업에서 잘 튜닝이 된 3세대 기법들에 비해 아직 비용 대비 성능이 압도적으로 우월하다고 하기에는 이른 단계이지만, 상대적으로 높은 정확도를 보여준다는 점에서 점차 현업에 적용이 확대되는 추세이다.

2015년 이후로는 모바일게임들에 “자동전투” 와 같은 기능들을 공식적으로 제공하기 때문에 더더욱 게임봇과 정상적인 사용자를 구분하는 것이 힘들어지고 있으므로, 더욱 오탐을 줄이고 정밀한 탐지를 해야하는 수요가 증가하고 있다. 현재 온라인게임은 예전보다 더욱 높은 정확도를 추구할 수 밖에 없는 환경으로 변화해가고 있으며, 이에 딥러닝 기술을 적극 도입하는 것이 좋은 대안이 될 수 있을 것으로 판단된다.

또한, Park 등의 연구 [52]에서 보듯이, 게임 종류 불문 게임 내 부정이용자들의 궁극적인 목적은 금전적 이익을 획득하는 것이라는 점을 고려해 보면, 딥러닝 알고리즘 (예: LSTM) 을 모든 피처에 적용하여 분석하는 것이 아닌 게임 내 거래에 특화하여 탐지하는 방식은 딥러닝 알고리즘의 비용을 줄여주면서도 높은 탐지력을 얻을 수 있는 좋은 방식이라 판단된다. 향후에도 도메인 지식과 결합하여 더욱 시너지를 내는 형태의 딥러닝 연구들이 온라인게임 보안 분야에서 데이터기반 보안 기법으로 활성화 될 것으로 예상된다.

### 4.2. 계정도용 탐지 분야의 재활성화

COVID-19 시대를 맞아 온라인게임 이용자 층이 더욱 증가하고 있다. 또한 온라인게임 내 가상 재화는 현금성 가치를 갖는 자산들이기 때문에, 해커들이 금전적 이익을 얻기 위해 온라인게임 이용자들의 계정을 탈취하는 공격 (Credential Stuffing)이 더욱 증가하고 있는 추세이다.

분석에 투입될 수 있는 기업의 리소스가 제한적인 경우, 게임봇 탐지와 계정도용 두 가지의 주요 위협 중에서 더 높은 우선순위를 부여하여 대응을 해야 하는 위협을 꼽으라면 계정도용을 꼽을 수 있겠다.

계정이 탈취될 경우 단순히 게임 내 자산에 대해서만 피해를 보는 것이 아니라 회원가입정보 등 개인정보가 유출되어 가상세계가 아닌 현실세계에 피해를 줄 수 있기 때문이다.

이러한 점을 고려해 볼 때 [38], [56] 와 같이 계정도용 탐지에 머신러닝을 적용하여 계정 탈취 공격에 대응을 하는 기술들에 대한 수요는 향후 꾸준히 증가할 것으로 예상된다.

## Ⅴ. 결 론

온라인게임은 2000년대 초반부터 중국발 해킹, 계정도용, 악성코드, 게임봇, 작업장과 같은 보안 문제들로 인해 정보보안기술의 최전선에 있어왔다. 더불어, 온라인게임은 태생적으로 대규모의 이용자들의 접속을 처리하며, 대량의 로그데이터 분석이 업무에 필수적인 사업영역인 온라인게임은 데이터기반 보안 영역이 일찍부터 성장한 분야라 할 수 있다.

그간 온라인게임에서 적용되어 왔던 데이터기반 보안기법들을 살펴보고, 향후 온라인게임 분야의 데이터

기반 보안이 어떠한 방향으로 발전해 나갈 것인가를 조망해 보았다. 본고에서 살펴본, 온라인게임 분야에서의 적용 사례 및 향후 조망은 간편송금, 온라인결제, 가상화폐거래소 등과 같이 대규모의 이용자들의 대량 데이터를 분석해서 높은 정확도로 대응해야 하는 다른 산업군에도 충분히 적용할 수 있을 것으로 기대된다.

## 참 고 문 헌


[1] Jeff Yan, “Security design in online games,” Computer Security Applications Conference, pp. 286-295, Dec. 2003

[2] Jiyoung Woo, and Huy Kang Kim, “Survey and research direction on online game security,” Proceedings of the Workshop at SIGGRAPH Asia, pp. 19-25, Nov. 2012

[3] Yuuki Mishima, Kenji Fukuda, and Hiroshi Esaki, “An analysis of players and bots behaviors in MMORPG,” Advanced Information Networking and Applications, pp. 870-876, Mar. 2013

[4] Fujita Atsushi, Hiroshi Itsuki, and Hitoshi Matsubara, “Detecting Real Money Traders in MMORPG by Using Trading Network,” AIIDE, Oct. 2011

[5] Ahmad, M. A., Keegan, B., Sullivan, S., Williams, D., Srivastava, J., and Contractor, N., “Illicit bits: Detecting and analyzing contraband networks in Massively Multiplayer Online Games,” Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing, pp. 127-134, Oct. 2011

[6] Kuan-Ta Chen and Li-Wen Hong, “User identification based on game-play activity patterns,” ACM SIGCOMM workshop on Network and system support for games, pp. 7-12, Sep. 2007

[7] Varvello Matteo and Geoffrey M. Voelker, “Second life: a social network of humans and bots,” Proceedings of the 20th international workshop on Network and operating systems support for digital audio and video, pp. 9-14, June 2010

[8] Mitterhofer Stefan, Platzer Christian, Kruegel Christopher and Kirda Engin, “Server-side bot detection in massive multiplayer online games,” IEEE Security and Privacy, pp. 29-36, Vol. 7, No. 3, May 2009

[9] Jina Lee, Jiyoun Lim, Wonjun Cho and Huy Kang Kim, “In-Game Action Sequence Analysis for Game BOT Detection on the Big Data Analysis Platform,” Proceedings of the 18th Asia Pacific Symposium on Intelligent and Evolutionary Systems, Vol. 2, pp. 403‑414, Jan. 2015

[10] Su-Yang Yu, Nils Hammerla, Jeff Yan, and Peter Andras, “Aimbot detection in online fps games using a heuristic method based on distribution comparison matrix,” Neural Information Processing, pp. 654-661, Jan. 2012

[11] Oh Jehwan, Zoheb Hassan Borbora and Jaideep Srivastava, “Automatic detection of compromised accounts in mmorpgs,” 2012 International Conference on Social Informatics, pp. 222-227, Dec. 2012

[12] Ah Reum Kang, Jiyoung Woo, Juyong Park, and Huy Kang Kim, “Online game bot detection based on party-play log analysis,” Computers & Mathematics with Applications, Vol. 65, No. 9, pp. 1384-1395, May 2013

[13] Mee Lan Han, Jung Kyu Park and Huy Kang Kim, “Online Game Bot Detection in FPS Game,” Proceedings of the 18th Asia Pacific Symposium on Intelligent and Evolutionary Systems-Volume, Vol. 2, pp. 479-491, Jan. 2015

[14] Platzer Christian, “Sequence-based bot detection in massive multiplayer online games,” Information, Communications and Signal Processing, pp. 1-5, Dec. 2011

[15] Roy Atanu, Ahmad Muhammad Aurangzeb, Sarkar CHandrima, Keegan Brian and Srivastava Jaideep, “The ones that got away: False negative estimation based approaches for gold farmer detection,” Privacy, Security, Risk and Trust, pp. 328-337, Sep. 2012

[16] Yeounoh Chung, Chang-young Park, Noo-ri Kim, Hana Cho, Taebok Yoon, Hunjoo Lee and

Jee-Hyong Lee, “Game Bot Detection Approach Based on Behavior Analysis and Consideration of Various Play Styles,” ETRI Journal, Vol. 35, No. 6, pp. 1058-1067, 2013

[17] Ahmad Mohd Ashraf, Keegan Brian, Roy Atanu, Dmitri Williams, Srivastava Jaideep and Contractor Noshir, “Guilt by association? Network based propagation approaches for gold farmer detection,” Advances in Social Networks Analysis and Mining, pp. 121-126, Aug. 2013

[18] Jehwan Oh, Borbora Zoheb Hassan, Sharma Dhruv and Srivastava Jaideep, “Bot Detection Based on Social Interactions in MMORPGs,” Social Computing, pp. 536-543, Sep. 2013

[19] Alayed Hashem, Fotos Frangoudes and Clifford Neuman, “Behavioral-based cheating detection in online first person shooters using machine learning techniques,” Computational Intelligence in Games, pp. 1-8, Aug. 2013

[20] McDaniel Ryan, and Roman V. Yampolskiy, “Development of embedded CAPTCHA elements for bot prevention in fischer random chess,” International Journal of Computer Games Technology, Vol. 2012, No. 2, Jan. 2012

[21] Su-Yang Yu, Hammerla Nils and Andras Peter, “A statistical aimbot detection method for online FPS games,” The International Joint Conference on Neural Networksm, pp. 1-8, June 2012

[22] Ruck Thawonmas, Yoshitaka Kashifuji, and Kuan-Ta Chen, “Detection of MMORPG bots based on behavior analysis,” International Conference on Advances in Computer Entertainment Technology, pp. 91-94, Dec. 2008

[23] Kuan-Ta Chen, Hsing-Kuo Kenneth Pao and Hong-Chung Chang, “Game bot identification based on manifold learning,” ACM SIGCOMM Workshop on Network and System Support for Games, pp. 21-26, Oct. 2008

[24] Steven Gianvecchio, Zhenyu Wu, Mengjun Xie and Haining Wang, “Battle of botcraft: fighting bots in online games with human observational proofs,” ACM conference on Computer and communications security, pp. 256-268, Nov. 2009

[25] Hyungil Kim, Sungwoo Hong and Juntae Kim, “Detection of auto programs for MMORPGs,” Advances in Artificial Intelligence, pp. 1281-1284, Dec. 2005

[26] Ah Reum Kang, Huy Kang Kim and Jiyoung Woo, “Chatting pattern based game BOT detection: do they talk like us?,” TIIS, Vol. 6, No. 11, pp. 2866-2879, 2012

[27] Hyukmin Kwon, Kyungmoon Woo, Hyun-chul Kim, Chong-kwon Kim and Huy Kang Kim, “Surgical strike: A novel approach to minimize collateral damage to game BOT detection,” Workshop on Network and Systems Support for Games, pp. 1-2, Dec. 2013

[28] Sang-Hyun Park, Hey-Wuk Jung, Sung-Woo Bang and Jee-Hyong Lee, “Game behavior pattern modeling for game bots detection in MMORPG,” International Conference on Uniquitous Information Management and Communication, pp. 33, Jan. 2010

[29] Jina Lee, Jiyoun Lim, Wonjun Cho and Huy Kang Kim, “I know what the BOTs did yesterday: Full action sequence analysis using Naïve Bayesian algorithm,” Annual Workshop on Network and Systems Support for Games, pp. 1-2, Dec. 2013

[30] Muhammad Aurangzeb Ahmad, Brian Keegan, Jaideep Srivastava, Dmitri Williams and Noshir Contractor, “Mining for gold farmers: Automatic detection of deviant players in mmogs,” Computational Science and Engineering, Vol. 4, pp. 340-345, Aug. 2009

[31] S.F.Yeung, John C.S.Lui, Jiangchuan Liu and Jeff Yan, “Detecting cheaters for multiplayer games: theory, design and implementation,” Proc IEEE CCNC, Vol. 6, pp. 1178-1182, Jan. 2006

[32] Roman V. Yampolskiy and Venu Govindaraju, “Embedded noninteractive continuous bot detection,” Computers in Entertainment, Vol. 5, No. 4, 2008

[33] Jiyoung Woo, Hwa Jae Choi and Huy Kang Kim, “An automatic and proactive identity theft de-

tection model in MMORPGs," Appl. Math, Vol. 6, No. 1, pp. 291-302, 2012

[34] Hsing-Kuo Pao, Hong-Yi Lin, Kuan-Ta Chen and Junaidillah Fadlil, "Trajectory based behavior analysis for user verification," Intelligent Data Engineering and Automated Learning - IDEAL, Vol. 6283, pp. 316-323, 2010

[35] Christensen Johanne, Oleg Veryovka and Ben Watson, "Win, lose or cheat: The analytics of player behaviors in online games," North Carolina State University, 2013

[36] Kyungmoon Woo, Hyukmin Kwon, Hyun-chul Kim, Chong-kwon Kim and Huy Kang Kim, "What can free money tell us on the virtual black market?," ACM SIGCOMM Computer Communication Review Vol. 41, No. 4, pp. 392-393, Aug. 2011

[37] Hyukmin Kwon and Huy Kang Kim, "Self-similarity based bot detection system in mmorpg," Proceedings of the 3th International Conference on Internet, pp. 477-481, Dec. 2011

[38] Hwa Jae Choi, Ji Young Woo and Huy Kang Kim, "Detecting Account Thefts on the Server-Side by Analyzing Game Log in MMORPGs," Proceedings of the 3th International Conference on Internet, pp. 501-506, Dec. 2011

[39] Dongnam Seo and Huy Kang Kim, "Detecting Gold-farmers' Groups in MMORPG by connection information," Proceedings of the 3th International Conference on Internet, pp. 583-588, Dec. 2011

[40] Kim, H.K. and Woo, J., 2019. Detecting and Preventing Online Game Bots in MMORPGs.

[41] Sylvain Hilaire, Hyun-chul Kim and Chong-kwon Kim, "How to deal with bot scum in MMORPGs?," Communications Quality and Reliability, pp. 1-6, June 2010

[42] Kim, Hana, Byung Il Kwak, and Huy Kang Kim. "A study on the identity theft detection model in MMORPGs." *Journal of The Korea Institute of Information Security & Cryptology* 25, no. 3 (2015): 627-637.

[43] Sungwoo Hong, Hyungil Kim and Juntae Kim, "Identification of Auto Programs by Using Decision Tree Learning for MMORPG," Journal of Korea Multimedia Society, Vol. 9, No. 7, pp. 927-937, July 2006

[44] Philippe Golle and Nicolas Ducheneaut, "Preventing bots from playing online games," Computers in Entertainment, Vol. 3, No. 3, pp. 3-3, July. 2005

[45] Kesteren Marlieke Van, Jurriaan Langevoort and Franc Grootjen, "A step in the right direction: Botdetection in MMORPGs using movement analysis," Proceedings of the 21st Belgian-Dutch Conference on Artificial Intelligence, Oct. 2009

[46] Kang, A. R., Jeong, S. H., Mohaisen, A., & Kim, H. K. (2016). Multimodal game bot detection using user behavioral characteristics.갽pringerPlus, 5(1), 523.

[47] Kwon, Hyukmin, et al. "Surgical strike: A novel approach to minimize collateral damage to game BOT detection." Proceedings of Annual Workshop on Network and Systems Support for Games. IEEE Press, 2013.

[48] Lee, E., Woo, J., Kim, H., & Kim, H. K. (2018). No Silk Road for Online Gamers!: Using Social Network Analysis to Unveil Black Markets in Online Games. In Proceedings of the 2018 World Wide Web Conference on World Wide Web (pp. 1825-1834). International World Wide Web Conferences Steering Committee.

[49] Chun, S., Choi, D., Han, J., Kim, H. K., & Kwon, T. (2018, April). Unveiling a Socio-Economic System in a Virtual World: A Case Study of an MMORPG. In Proceedings of the 2018 World Wide Web Conference on World Wide Web (pp. 1929-1938). International World Wide Web Conferences Steering Committee.

[50] Kwon, Hyukmin, et al. "Crime Scene Reconstruction: Online Gold Farming Network Analysis." IEEE Transactions on Information Forensics and Security (2016).

[51] E. Lee, J. Woo, H. Kim, A. Mohaisen, and H.

K. Kim, “You Are a Game Bot!: Uncovering Game Bots in MMORPGs via Self-similarity in the Wild,” NDSS 2016.

[52] Park, Kyung Ho, Eunjo Lee, and Huy Kang Kim. “Show Me Your Account: Detecting MMORPG Game Bot Leveraging Financial Analysis with LSTM.” In *International Workshop on Information Security Applications*, pp. 3-13. Springer, Cham, 2019.

[53] Ki, Youngjoon, Jiyoung Woo, and Huy Kang Kim. “Identifying spreaders of malicious behaviors in online games.” Proceedings of the companion publication of the 23rd international conference on World wide web companion. International World Wide Web Conferences Steering Committee, 2014.

[54] Woo, Jiyoung, Ah Reum Kang, and Huy Kang Kim. “Modeling of bot usage diffusion across social networks in MMORPGs.” Proceedings of the Workshop at SIGGRAPH Asia. ACM, 2012.

[55] Woo, Jiyoung, Ah Reum Kang, and Huy Kang Kim. “The contagion of malicious behaviors in online games.” ACM SIGCOMM Computer Communication Review 43.4 (2013): 543-544.

[56] Kim, Hana, Seongil Yang, and Huy Kang Kim. “Crime scene re-investigation: a postmortem analysis of game account stealers' behaviors.” In *2017 15th Annual Workshop on Network and Systems Support for Games (NetGames)*, pp. 1-6. IEEE, 2017.

[57] Xu, J., Luo, Y., Tao, J., Fan, C., Zhao, Z. and Lu, J., 2020. NGUARD+ An Attention-based Game Bot Detection Framework via Player Behavior Sequences. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, *14*(6), pp.1-24.

## 〈저자소개〉

**김 휘 강 (Huy Kang Kim)**

종신회원

1998년 2월 : KAIST 산업경영학과 학사

2000년 2월 : KAIST 산업공학과 석사

2009년 2월 : KAIST 산업및시스템공학과 박사

2004년 5월~2010년 2월 : 엔씨소프트 정보보안실장, Technical Director

2010년 3월~2015년 2월 : 고려대학교 정보보호대학원 조교수

2015년 3월~2020년 2월 : 고려대학교 정보보호대학원 부교수

2020년 3월~현재 : 고려대학교 정보보호대학원 교수

<관심분야> 온라인게임 보안, 자동차 보안, 네트워크 보안, Cyber Threat Intelligence