

# 온라인 게임 내의 부정 행위 탐지 연구 동향

우지영\*, 김휘강\*\*

## 요약

온라인 게임은 가상 재화를 현금화할 수 있게 되면서 여러 가지 부정 행위가 발생하고 있다. 그 중 대표적인 것이 사용자 대신에 게임 플레이를 해주는 게임 봇(game bot)이다. 이러한 게임 봇은 사용자는 물론 게임회사에 큰 해를 입히고 있다. 본 연구에서는 게임 봇을 탐지하는 기존의 연구 중 사용자의 행동 로그를 분석하는, 데이터 분석 기반의 연구를 조사하였다. 관련 연구를 사용자의 행위를 중심으로 구분하였고, 향후 연구가 나아갈 방향에 대해 첨언하였다.

## I. 서론

온라인게임은 인터넷 역사상 WWW (World Wide Web)과 더불어 가장 성공적인 인터넷 응용서비스 중 하나로 자리매김하고 있다 [1]. 최근 10년간 국내외 온라인게임 시장은 꾸준한 성장세를 보여 왔으며, 스마트폰 및 태블릿 기기의 보급 확산으로 인해 모바일 게임 역시 급성장하고 있다. 게임 시장의 비약적인 성장과 함께 온라인게임과 관련된 보안 위협 역시 급증하고 있다. 게임은 국가기반시설이나 금융권, 전자상거래 서비스보다 상대적으로 정부의 기술적, 관리적 보안 가이드라인은 약한데 비해 해킹이 발생하였을 경우 해커가 얻을 수 있는 이익이 크기 때문이다. 해킹에 성공할 경우 대규모 사용자들의 고객 개인정보 외에도 온라인게임 아이템을 조작하거나 더 나아가 이를 현금화할 수 있다는 점에서 해커들에게 매력적인 공격대상으로 여겨지고 있다. 이들은 직접 해킹을 시도하기도 하고, 불법 프로그램을 만들어 일반인에게 유통하기도 한다. 불법 프로그램의 대표적인 것은 게임 봇으로 사람대신에 게임을 하게해주는 자동 봇이다. 게임 봇은 개인 사용자가 사용하기도 집단이 사용하기도 한다.

더욱이 온라인 게임에서 가상 재화를 현금화할 수 있으므로 지하경제의 형성에도 큰 영향을 미친다. 게임 내의 사이버 재화를 현금으로 바꾸는 행위인 현금거래는 작업장이라고 불리는 전문적인 부정 사용자 조직에 의해 이루어지는데, 작업장의 현금거래는 탈세나 돈세탁

등과 같은 실물경제의 범죄활동과 연관되고 있다[2].

게임 내 이러한 부정 행위를 탐지하는 방법은 여러 방법이 있는데, 그 중 최근에 주목을 받고 있는 것이 데이터 분석 기반의 방식이다.

부정 행위를 방지하는 방법은 사전에 부정 행위를 차단하는 것이다. 그 첫 번째가 사용자가 불법 프로그램을 사용하는지를 감시하는 소프트웨어를 클라이언트에서 작동하게 하는 방식이다. 이러한 방식은 사용자의 불편을 일으키고, 우회 가능하다는 단점을 가진다. 또한, 설치된 소프트웨어가 모든 불법 소프트웨어를 감시할 수 있는 것도 아니다 [3].

두 번째는 사용자의 네트워크를 감시하는 방식이다. 네트워크 상에서 이상한 트래픽이 발생하는지를 모니터링 하는 방식인데, 이러한 방식은 전송 데이터에 암호화를 적용한 경우 서버의 부하를 유발하는 단점이 있다 [4].

이와는 반대로 사후 처리 방식이 있는데, 이는 데이터 기반으로 증거를 획득한 후 증거를 이용해 이상 사용자를 추출하는 방식이다. 게임 내 사용자의 행동을 분석하기 위해서 게임회사에서는 사용자의 행위를 로그화하여 기록하고 있다.

이 기록을 이용하면 고객관리, 아이템 판매, 이상 사용자 탐지 등에 활용할 수 있다. 이러한 방식을 기존에 구축된 데이터를 이용한다는 장점이 있고, 사용자의 클라이언트 PC나 네트워크에 부하를 주지 않아 정상 사용자의 불편을 최소화하는 장점이 있다. 또한 다방면의

\* 순천향대학교 (jywoo@sch.ac.kr)

\*\* 고려대학교 (cenda@korea.ac.kr)

분석을 통해 다양한 이상징후를 찾아낼 수도 있다. 또한 데이터 분석을 통한 이상징후 탐지는 알려진 위험을 사전에 방지하는 방식이 모든 위험에 대응하기 어려우므로 100% 방어가 되지 않는다는 점을 해결해준다.

본 논문에서는 데이터 분석 기반 이상 사용자 탐지에 대한 연구의 흐름을 정리하고, 관련 연구자들에게 향후 연구 방향을 제시하고자 한다. 이를 위해 사용자의 행위와 소셜 네트워크 관점으로 기존의 논문을 정리하여 소개한다.

## II. 게임 붏과 작업장

일부 게임 사용자는 충분히 노력하지 않고 쉽고 빠르게 레벨을 올리려고 부정 행위를 한다. 게임 아이템과 게임 머니는 파워와 명성을 향상시켜 게임 캐릭터의 생존 가능성을 높이는 데 중요하다. 특히 MMORPG (Massively Multiplayer Online Role-Playing Game)는 플레이어가 높은 수준의 캐릭터를 얻고 사이버 자산이 축적하도록 사전에 계획된 과정을 거쳐야 하도록 설계되어 있다. 이 코스는 반복적인 플레이에 많은 시간을 할애해야한다. 리니지 (Lineage)의 경우 사용자는 최고 수준에 도달하기 위해 2.5 시간 동안 하루에 3 시간 씩 소비해야한다고 한다 [5]. 이러한 시간 소모적인 프로세스를 건너 뛰고 짧은 시간 내에 더 많은 사이버 자산을 확보하기 위해 사용자는 부정 행위를 하기 시작했다.

온라인 게임에서의 부정 행위는 이제는 사용자 사적인 문제가 아니며, 온라인 게임은 대규모 플레이어를 유지하고 단일 플레이어 게임을 넘어서 플레이어 간의 사회적 활동을 형성하기 때문에 다른 플레이어에게 피해를 준다.

온라인 게임에서 가장 많이 사용되는 도구는 게임 붏이다. 게임 붏의 전형적인 유형은 인간을 대신에 게임을 하는 자동 프로그램이다.

게임 붏은 게임 플레이 규칙을 임의로 변경하고, 다른 사용자를 부당하게 패배시키며, 불공정한 이익을 취득한다.

게임 붏은 게임 플레이를 가속하며, 벽을 통해보고, 불법으로 텔레포트하고, 승자로 위조된 리포트를 주는 등의 다양한 기능을 갖추고 있다. 게임 붏은 자동으로 표적을 탐지하고 표적을 인간보다 빨리 죽일 수 있다. 또한, 휴식 없이 훨씬 더 오랫동안 게임을 할 수 있다.

붏의 이러한 행동은 다른 사용자들에게 눈에 띄기 때문에 사용자를 부당하게 느끼게 하고 사용자가 게임을 떠나는 원인이 될 수 있다 [6,7].

회사 차원에서는 게임 붏은 사용자가 게임 아이템과 게임 머니를 구매하지 않고 게임을 하게 하므로 이러한 고객은 손해이다. 또한, 사용자가 게임 붏을 사용하면 게임 디자이너가 예상한 것보다 짧은 시간 내에 최대 레벨에 도달 하게 하는데, 최대 레벨의 사용자는 게임을 즐기고 나갈 더 이상 게임 내용이 없게 되어 게임을 떠나게 된다. 즉, 아이템 판매량과 사용자 수를 줄이고 게임 라이프 사이클을 단축시킨다. Castronova [7]는 게임 붏이 게임회사에 끼치는 손해를 추정하였다. WoW(World of Warcraft)의 경우 연간 1,800만 달러로 손해가 있다고 밝혔다.

## III. 게임에서 이상행위 탐지 연구 분류

게임 내 사용자의 행동을 분석하기 위해서 게임회사에서는 사용자의 행위를 로그화하여 기록하고 있다. 사용자별 개별 행동을 분석하면 이상 행위와 일반 게임 플레이는 차이를 보인다. 초기 연구는 개개인의 플레이 패턴을 주로 관찰하였다. 그 후에는 MMORPG의 특징을 살려 사용자의 다른 사용자와의 상호작용을 이용하는 연구가 제시되었다.

소셜행동을 분석을 하게 되면, 사기행위를 하는 사람들의 반사회적 성향을 볼 수 있을 것이라는 점에 착안한 것이다.

MMORPG는 혼자 게임을 하는 것보다는 여럿이 협동하여 어려운 작업을 해결할 수 있도록 디자인되어 있다. 특히 이 종류의 게임은 이러한 사회적 작용을 통해 사용자의 몰입감을 높이고, 이탈을 방지하는 역할을 하게 된다. 사회적 활동을 보면 게임 붏 사용자는 일반 사용자에 비해 일반인들과의 상호작용이 적다.

상호작용을 살펴보면, 이를 네트워크(또는 그래프) 형태로 구현할 수 있다. 네트워크를 구성하게 되면 정상과 부정 행위자의 두 집단의 네트워크를 구분할 수도 있고, 전체 네트워크 상에서 두 집단이 위치한 특징을 찾아낼 수도 있다. 마지막으로 네트워크가 구성되면 그 안에서 일어나는 일을 기술하고 예측할 수 있다.

### 3.1. 개별 행위 관점

사용자의 행위를 기록하는 로그를 이용해서 봇과 일반 사용자를 구분하는 것은 두 그룹에서 유의하게 차이는 로그를 도출하는 것이 필요하다. 로그의 종류의 차이나 로그의 분포의 차이를 도출하여 탐지 모델을 만든다.

많은 연구에서 봇과 사용자의 차이점을 찾아내려고 노력하였다. Kesteren 외 [8], Mitterhofer 외 [9], Chen 외 [10]의 연구에서는 사용자의 이동패턴을 분석하여, 정상 사용자와 봇을 구분하였다. 이들의 연구에서는 일반 사용자의 이동패턴이 규칙적이지 않지만 봇은 그 움직임이 프로그래밍 되어 있어 일정하다는 점에 착안했다.

게임 봇은 사람들이 하기 귀찮은 작업을 장시간 할 수 있으므로 이러한 차이점에 집중한다면, 게임 봇 탐지 모델을 만들 수 있다.

Ruck 외 [11]의 연구는 행위 빈도를 통해 게임 봇을 탐지하였다. Chung 외 [12]의 연구에서는 다양한 플레이 패턴을 분석하고, 사용자의 전투력과 아이템 수집력, 이동성 등을 변수화하여 봇과 일반 사용자를 구분하는 모델을 제안하였다.

Zhang 외 [13]의 연구에서는 문서를 군집화하는 topic model을 이용하여 사용자의 게임 시간과 레벨을 변수로 사용하였다.

게임 봇은 프로그램이기 때문에 행동이 기계적일 것이라는 점에 착안하여 Chen과 Hong [14]의 연구에서는 사용자 행위 사이의 쉬는 시간 (idle time) 존재 여부를 이용하였다.

게임 봇의 대표적인 특징은 장시간 동일 작업을 계속 한다는 것이다. 이러한 성질을 이용하여 변수(feature)를 만드는 방법이 있다.

로그의 반복성을 자기 유사성(self-similarity)으로 변수화하여 자기 유사성이 높은 사용자가 봇임을 밝히는 연구가 발표되었다 [15]. Idle time이나 자기 유사성 변수가 갖는 장점은 게임 종류에 상관없이 적용가능하다는 것이다. 게임 봇에서 주로 나타나는 행위 로그를 선정한 뒤에 행위의 반복성을 측정하기 때문에 게임 종류에 상관없이 적용할 수 있다.

더 나아가면 반복되는 행위 자체를 분석할 수 있다. 이 경우에는 대응량의 컴퓨팅 용량이 필수적이기 때문

에 빅데이터 처리 플랫폼이 필요하다.

이어나 외 [16]의 연구에서는 NCsoft사에서 구축된 빅데이터 처리 시스템을 이용하여, 사용자의 행동을 시퀀스로 나타내어 정상 사용자와 부정 사용자의 행동을 구분하는 시퀀스를 찾아내는 방법을 제안하였다.

하지만 이 방법은 게임사용자가 다양하므로, 특히, 게임 봇처럼 장시간 반복되는 플레이를 직접 하는 사용자도 존재하기 때문에 다양한 사용자의 행동을 일반화하여 봇과의 차이를 구별하기는 쉽지 않다.

### 3.2. 상호작용(소셜) 행위 관점

게임 내에서의 사용자의 소셜행위는 친분을 위한 것과 목적성 행위로 나눌 수 있다. 친분을 위한 행위는 친구를 맺거나 커뮤니티를 형성하는 것이 해당하고, 목적성 행위는 게임 내에서 게임 플레이를 같이 한다가거나 아이템을 거래한다거나 대화를 한다거나 등의 필요에 의해 만들어지는 것을 의미한다.

친구나 길드(커뮤니티)와 같은 관계의 친분 목적의 관계를 매개로 팀플레이, 거래, 대화 등의 목적성 관계가 이루어질 수 있다.

소셜 행위 관점은 사람은 다양한 사회적 활동을 하지만 게임 봇은 재화를 직접 얻을 수 있는 행위에만 가중하는 특징을 가진다. 게임 봇은 굳이 다른 사용자와 친구 관계를 맺거나 커뮤니티에 가입하여 활동하지 않을 것이다.

반면에 게임 봇도 파티를 맺어 팀플레이를 하거나 대화를 하고, 채굴한 아이템을 파는 활동은 한다. 강아름 외 연구 [17]에서는 게임 봇의 파티 활동, 대화의 행위가 일반 사용자와 어떻게 다른지를 분석하였다. 강아름 외 [18]의 연구에 따르면 게임 봇도 팀을 이루어 게임 플레이를 하는데, 팀을 이루는 방식과 팀을 이룬 후 하는 행위가 차이를 보인다. 게임 봇은 특정 몇 명의 캐릭터와 팀을 맺는데, 주로 이들도 게임 봇이며, 이들은 아이템 채굴을 효율적으로 하기 위해 역할 분담을 한다. 한 명은 아이템을 채굴하고, 한명은 몬스터의 공격을 살피고 대응하는 역할을 한다.

또한 강아름 외 [18]의 또 다른 연구에서는 게임 봇은 대화방식에서도 일반 사용자와 차이를 나타냄을 보여주었다. 우선 일반사용자는 봇 사용자보다 대화량이 현저히 많았다. 또한 일반 사용자는 다른 사용자와 다양

한 대화를 하는 반면 게임 붓은 사람의 언어가 아닌 사람이 이해하기 어려운 대화를 하는 것으로 나타났다. 완전한 문장이 아닌 특정 문자를 반복적으로 보여주는 것도 게임 붓끼리의 대화의 특징이다.

Jeong 외 [20]의 논문에서는 붓과 사람의 소셜 행위의 차이를 분석하였다. 이 연구에 따르면 붓과 사람은 친구를 맺는 정도는 크게 다르지 않지만, 거래는 많고, 대화나 메일을 보내는 활동은 사람보다 낮은 것으로 나타났다.

이재혁 외 [20]의 논문에서는 사용자의 행동을 Maslow [21]의 “욕구단계이론”에 따라 생리적 욕구, 안전의 욕구, 소속과 애정 욕구, 존경의 욕구, 자아실현 욕구로 구분하고, 붓과 사람을 구분하는데 이렇게 구분된 욕구를 사용하였다. 이 논문에서는 붓은 다른 사용자와의 상호작용에 해당하는 욕구가 적다는 것을 보이고, 이를 활용하면 붓을 탐지할 수 있음을 보였다.

### 3.3. 소셜 네트워크 관점

소셜행위를 관찰하고 나면 소셜 네트워크를 구축할 수 있다. 소셜행위의 두 주체를 노드로 둘 사이의 상호작용을 엣지로 형성하면 게임 내 사용자 사이의 네트워크를 구축할 수 있다.

개인이 형성한 네트워크의 구조는 그 집단의 특성을 나타낸다 [22]. 집단의 종류에 따라 다양한 네트워크를 형성하지만 네트워크를 관찰해보면 공통되는 특징을 찾을 수 있다.

이러한 점을 이용해서 범죄 조직을 그들의 관계를 네트워크 관점에서 분석한 연구가 선행되었다. Chen [23]의 연구를 살펴보면, 범죄 종류별 집단의 네트워크 특징이 다른 것을 알 수 있다. 마약, 조폭도 서로 다른 네트워크 특징을 가지고 있는 것으로 조사되었다. 네트워크의 특징은 네트워크의 구조와 네트워크 상에서의 노드의 특징을 의미한다.

Keegan 외 [24]와 LEHDONVIRTA [25]의 연구에서는 부정 행위 집단의 네트워크 구조의 특징을 기술하였다. Oh외 [26]의 연구에서는 멘토링 네트워크에 주목하고, 붓과 사람을 구분하기 위해 주변 사람들의 중요도로 나의 중요도를 측정하는 eigen vector centrality를 이용하였다.

Bernardi 외 [27]의 연구에서는 사용자가 취할 수 있

는 모든 상호작용을 바탕으로 전체 네트워크를 구성하고, 사용자의 행동과 네트워크 변수를 이용하여 붓을 구분하였다.

강아름 외 [28]의 논문에서는 사용자의 파티, 친구, 거래, 대화, 메일 등의 상호작용을 바탕으로 소셜 네트워크를 구성하고, 붓과 사람이 구성한 네트워크의 차이를 네트워크 구조 측면에서 찾아냈다. 또한, 붓끼리나 사람끼리만 말고, 붓과 사람도 관계를 맺을 수 있는데, 이의 차이도 분석하였다. 또한, 네트워크를 구성하는 작은 단위를 살펴보았는데, 붓은 일방적인 상호작용이 많은 반면에 사람은 쌍방향 상호작용이 많다는 것을 보여주었다.

Blackburn 외 [29]의 논문에서는 붓 사용자가 사용자의 네트워크 상에서 잘 녹아들어 있긴 하지만, 게임 커뮤니티 네트워크 상에서의 위치가 일반 사용자와 다르지는 않다고 말했다. 이 연구에서 사용한 게임 커뮤니티는 게임 내는 아니고, STEAM이라는 여러 종류의 게임을 할 수 있는 커뮤니티이다. 이 네트워크 상에서의 위상으로는 개인 사용자를 찾아내기는 어려운 것으로 보인다. Blackburn 외 [29]의 연구는 기존의 연구와 상반된 결론을 내긴 했지만, 이는 개인 사용자의 부정 행위를 찾는 것은 분석할 네트워크에 따라 다르다는 것을 말한다.

네트워크 위상을 이용하면, 집단으로 부정 행위를 하는 집단은 찾을 수 있다. 네트워크 관점으로 확장하면 개인 게임 붓이 아니라 게임 붓 집단을 찾을 수 있다. 게임 붓을 이용하면 재화 채굴이 손쉽고, 게임 내 재화는 게임시장 밖에서 현금화할 수 있으므로 게임 붓을 대규모로 운영하기도 한다. 이를 작업장이라고 부른다. 이들은 주로 자신들만의 네트워크를 형성하는데 이는 개별 사용자보다는 돈을 벌 목적으로 조직화된 집단이므로 폐쇄된 네트워크를 형성한다.

권혁민 외 [30]. 이은조 외 [31]의 연구에서 네트워크 관점에서 게임 붓과 작업장을 탐지하는 모델을 제시하였다. 이들은 작업장은 일반 사용자와는 다른 네트워크 구조를 형성하는 것을 발견하였다.

권혁민 외 [30]의 연구에서는 거래 관계에서 이상한 거래, 즉 대가없이 일어나는 거래에 주목하고, 일부 이상한 거래를 초기값으로 이들과 거래하는 사람들로 네트워크를 확장시켰다. 이렇게 찾아낸 몇몇의 네트워크 특징을 분석하여 다른 작업장도 찾아내는 모델을 제시

하였다. 이은조 외 [31]의 연구에서는 거래 네트워크를 구축하고, 네트워크를 특징이 비슷한 그룹 즉, 커뮤니티를 찾는 방식으로 주된 그룹과는 다른 그룹을 찾아 이들이 작업장임을 보였다.

김하량 외 [32]의 논문에서는 목적성 커뮤니티 성격이 강한 길드 네트워크에 주목하고, 붓이 형성하는 길드 네트워크와 사람이 형성하는 것의 차이를 도출하여 붓 길드를 탐지하는 연구를 수행하였다.

### 3.4. 네트워크 상에서의 확산의 관점

사용자의 소셜행위를 분석하고, 이들로 네트워크를 구성하게 되면, 네트워크 상에서 발생하는 현상을 관찰하고 예측할 수 있다. 사용자의 게임 내에서의 관계 네트워크가 구축되면 이 네트워크가 나쁜 행동을 전파시키는 통로 역할을 하기도 한다. 사용자의 채팅 내역을 살펴보면, 게임 붓의 경우, 친구 네트워크를 통해 유통되기도 한다. 친구 그룹에서 한명이 게임 붓을 구하거나 제작하여 친구들에게 소개하고 전달하기도 한다. 이러한 관찰 사실을 이용하여 게임 붓의 전파 과정을 모델링하고, 붓 사용자를 찾는 연구가 수행되고 있다.

우지영 외 [33]의 연구에서는 친구의 붓 사용이 나의 붓 사용에 영향을 미친다는 것을 보였다. 우지영 외 [34, 35]의 연구에서는 또한 게임 붓 전염에 적합한 모델을 제시하였다. 첫 번째 모델 [34]은 파티 네트워크에서 일회성 상호작용을 통해 붓이 전염될 가능성을 분석하고, 이를 통해 전체 중 몇 명이 붓에 감염될지를 예측하였다.

두 번째 모델 [35]은 해당 모델을 이용하여 친구 네트워크 상에서 전염의 확률을 구하고, 이를 바탕으로 붓 사용자를 추출하는 연구를 제안하였다.

이는 행동의 전염, 정보 전파의 연구가 게임 내 나쁜 행동에 적용된 것이다. 선한 행동, 유행이 전체 집단에서 퍼져나가는 현상을 기술하는 연구에서, 2단계는 네트워크 상에서 퍼져나가는 현상을 기술하고, 마지막으로 현상을 기술할 수 있는 모델을 개발한다. 이 모델을 이용하면 미래에 발생할 전염이나 전파를 예측할 수 있다.

2005년에 World of Warcraft라는 가상 세계 내에서 전염병이 발생하였다 [36]. 이는 오염된 피라는 주문에 걸리게 되면 캐릭터의 피가 감소하게 되는데, 이는 게임

사용자가 해제하기 어렵게 되어있었다. 이 주문은 전염성을 가지고 있어 사람들이 많이 모이는 곳에서 급속도로 확산되었다. 특히, 일부 사용자는 혼자 죽을 수 없다는 생각에 다른 사람들을 일부러 전염시키고 다니기도 했다. 이 현상은 네트워크를 타고 발생한 것은 아니고, 전체 인구(population)에서 발생한 것이다.

확산에 대한 연구는 크게 2단계로 이루어지는데, 1단계는 집단의 모든 사람이 그들의 관계와 상관없이 모든 사람이 접촉을 가질 수 있다는 것을 전제로 한다. 2단계 연구는 집단의 모든 사람이 접촉을 가진다는 전제를 깨고, 집단에 속하는 사람들은 그들이 가지는 네트워크를 통로로 전파가 이루어진다는 것이다. 첫 번째 단계를 인구 기반 모델이라고 하고, 두 번째를 네트워크 기반 모델이라고 한다. 온라인 게임 상에서도 확산의 관점을 인구 기반과 네트워크 기반으로 나눌 수 있다. 인구 기반 모델의 경우에는 전체 인구 중 몇 명이 감염되는지 등에 대해서는 예측할 수 있지만, 누가 감염될지를 탐지해 내기는 어렵다. 따라서 붓 사용자를 탐지하는 데는 적합하지 않다. 반면 네트워크 모델은 사용자별 네트워크 상에서 연결현황을 알 수 있으므로, 연결된 사용자의 붓 사용 여부를 기초로 해당 사용자의 붓 사용 확률을 도출할 수 있다.

Ahmad외 [37]의 연구에서는 label propagation 방식으로 작업장을 탐지하는 방법을 제안하였다. 해당 연구는 여러 작업장 간에 긴밀한 네트워크를 형성하고 있다는 점에 착안하여, 주변의 행동으로부터 특정인의 행동을 유추하는 방식이다. 본 연구에서는 활성화 값을 주어 label propagation을 진행하고, 이 값과 플레이패턴, 인구통계 값을 이용하여 분류기를 개발하였다.

## IV. 결 론

본 논문에서는 게임내의 부정 행위 탐지에 대한 연구를 조사하였다. 최근 보안 분야의 흐름인 데이터분석 기반 방법에 초점을 맞추어, 사용자의 행위를 중심으로 기존 연구를 구분하였다. 관련 분야 연구는 사용자의 단독 행위에 집중하다가 소셜 행위를 이용한 탐지 방법으로 방향이 전환되고 있다. 더 나아가 소셜 행위로부터 구축된 소셜 네트워크를 이용한 연구가 수행되고 있다. 소셜 네트워크를 구성하게 되면, 그 다음은 네트워크의 진화와 네트워크 상에서의 정보나 행동의 확산을 살펴볼 수

있다. 아직은 네트워크의 진화를 이용한 연구는 없으며, 네트워크 상에서의 정보의 확산을 이용하여 봇 사용을 예측하고 탐지하는 연구가 시작되고 있다. 봇과 사람이 생성하는 소셜 네트워크를 단적으로 보는 것이 아니라 시간에 따라 진화하는 양상을 이용한다면, 기존 연구와는 확연히 다른 연구가 될 것이다.

## 참 고 문 헌

- [1] Infiniti Research Limited. Global online gaming market 2014. <http://www.marketwatch.com/story/global-online-gaming-market-2014-2014-06-25>, 2014. (accessed on 14 October 2016).
- [2] E. Digital. Group laundered \$38m in virtual currencies in 18 months. <http://www.engagedigital.com/blog/2008/10/27/group-laundered-38m-in-virtual-currencies-in-18-months/>, 2008.
- [3] Jiyoung Woo, Huy Kang Kim. "Survey and research direction on online game security." Proceedings of the *Workshop at SIGGRAPH Asia*. ACM, 2012.
- [4] 광병일, 김휘강. "온라인 게임에서의 이상 징후 탐지 기법 조사 및 분류." 정보보호학회논문지 25.5 (2015): 1097-1114.
- [5] <http://boards.lineage2.com/>
- [6] Atsushi Fujita, Hiroshi Itsuki, and Hitoshi Matsubara. "Detecting Real Money Traders in MMORPG by Using Trading Network." AIIDE. 2011.
- [7] E. CASTRONOVA. Effects of botting on world of warcraft. [http://virtuallyblind.com/files/mdy/blizzard\\_msj\\_exhibit\\_7.pdf](http://virtuallyblind.com/files/mdy/blizzard_msj_exhibit_7.pdf), 2007.
- [8] Van Kesteren Marlieke, Jurriaan Langevoor, 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
- [9] Mitterhofer Stefan, Platzer Christian, Kruegel Christopher, Kirda Engin. "Server-side bot detection in massive multiplayer online games," *IEEE Security and Privacy*, pp. 29-36, Vol. 7, No. 3, 2009
- [10] Kuan-Ta Chen et al. "Game bot detection based on avatar trajectory." *International Conference on Entertainment Computing*. Springer, Berlin, Heidelberg, 2008.
- [11] Thawonmas Ruck, Yoshitaka Kashifuji, Kuan-Ta Chen. "Detection of MMORPG bots based on behavior analysis," *International Conference on Advances in Computer Entertainment Technology*, pp. 91-94, Dec. 2008
- [12] Yeounoh Chung et al. "Game bot detection approach based on behavior analysis and consideration of various play styles." *ETRI Journal* 35.6 (2013): 1058-1067.
- [13] Zhongqiang Zhang et al. "Detection of illegal players in massively multiplayer online role playing game by classification algorithms." *Advanced Information Networking and Applications (AINA), 2015 IEEE 29th International Conference on*. IEEE, 2015.
- [14] Kuan-Ta Chen, 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
- [15] Eunjo Lee et al. "You are a Game Bot!: Uncovering Game Bots in MMORPGs via Self-similarity in the Wild." NDSS. 2016.
- [16] Jina Lee, Jiyoum Lim, Wonjun Cho, Huy Kang Kim, "I know what the BOTs did yesterday: Full action sequence analysis using Naive Bayesian algorithm," *Annual Workshop on Network and Systems Support for Games*, pp. 1-2, Dec. 2013
- [17] Ah Reum Kang, Jiyoung Woo, Juyong Park, 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
- [18] Stefan Mitterhofer, Platzer Christian, Kruegel Christopher, Kirda Engin. "Server-side bot detection in massive multiplayer online games," *IEEE Security and Privacy*, pp. 29-36, Vol. 7,

- No. 3, 2009
- [19] Seong Hoon Jeong, Ah Reum Kang, Huy Kang Kim. "Analysis of Game Bot's Behavioral Characteristics in Social Interaction Networks of MMORPG." *ACM SIGCOMM Computer Communication Review*. Vol. 45. No. 4. ACM, 2015.
- [20] 이재혁, 강성욱, 김휘강. "모티베이션 이론을 이용한 온라인 게임 내 부정 행위 탐지." *한국게임학회 논문지* 15.4 (2015): 69-78.
- [21] A. H. Maslow. "A theory of human motivation," *Psychological Review*, vol. 50(4), pp.370-396, Jul 1943.
- [22] Mark Newman. *Networks: an introduction*. Oxford university press, 2010.
- [23] Hsinchun Chen. *Dark web: Exploring and data mining the dark side of the web*. vol. 30. *Springer Science & Business Media*, 2011.
- [24] Brian Keegan, et al. "Dark gold: Statistical properties of clandestine networks in massively multiplayer online games." *Social Computing (SocialCom), 2010 IEEE Second International Conference on*. IEEE, 2010.
- [25] Vili. Lehdonvirta. "Real-money trade of virtual assets: new strategies for virtual world operators." (2008).
- [26] Jehwan Oh. "Bot detection based on social interactions in MMORPGs." *Social Computing (SocialCom), 2013 International Conference On*. IEEE, 2013.
- [27] Mario Luca Bernardi et al. "A time series classification approach to game bot detection." *Proceedings of the 7th International Conference on Web Intelligence, Mining and Semantics*. ACM, 2017.
- [28] Ah Reum Kang et al. "Multimodal game bot detection using user behavioral characteristics." *SpringerPlus* 5.1 (2016): 523.
- [29] Jeremy Blackburn et al. "Cheating in online games: A social network perspective." *ACM Transactions on Internet Technology (TOIT)* 13.3 (2014): 9.
- [30] Hyukmin Kwon et al. "Crime scene reconstruction: Online gold farming network analysis." *IEEE Transactions on Information Forensics and Security* 12.3 (2017): 544-556.
- [31] Eunjo Lee, Jiyoung Woo, Hyungshick Kim, Huy Kang Kim, "Show me the black money!: Analysis of Real Money Trading Network in MMORPG", Working paper.
- [32] 김하량, 김휘강. "온라인 게임 봇 길드 탐지 방안 연구." *정보보호학회논문지* 25.5 (2015): 1115-1122.
- [33] Jiyoung Woo, Ah Reum Kang, and Huy Kang Kim. "The contagion of malicious behaviors in online games." *ACM SIGCOMM Computer Communication Review*. Vol. 43. No. 4. ACM, 2013.
- [34] Jiyoung Woo, 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.
- [35] Jiyoung Woo. "Contagion of Cheating Behaviors in Online Social Networks", Working paper.
- [36] [https://en.wikipedia.org/wiki/Corrupted\\_Blood\\_in\\_cident](https://en.wikipedia.org/wiki/Corrupted_Blood_in_cident)
- [37] Muhammad Aurangzeb Ahmad et al. "Guilt by association? Network based propagation approaches for gold farmer detection." *Advances in Social Networks Analysis and Mining (ASONAM), 2013 IEEE/ACM International Conference on*. IEEE, 2013.

<저자 소개>



**우 지 영 (Jiyoung Woo)**  
정회원

2000년 2월: KAIST 산업공학과 학사  
2002년 2월: KAIST 산업공학과 석사  
2006년 2월: KAIST 산업공학과 박사  
2006년 3월~2008년 9월: 삼성화재  
CRM파트 과장

2008년 10월~2010년 10월: 미국 아  
리조나대학 인공지능연구실 연구원

2011년 2월~2016년 8월: 고려대 학교 정보보호대학원 연  
구교수

2016년 9월~현재: 순천향대학교 빅 데이터공학과 조교수  
관심분야: 데이터마이닝



**김 휘 강 (Huy Kang Kim)**  
증신회원

1998년 2월: KAIST 산업경영학과  
학사

2000년 2월: KAIST 산업공학과 석사

2009년 2월: KAIST 산업및시스템  
공학과 박사

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

2010년 3월~2015년 2월: 고려대학교 정보보호대학원 조  
교수

2015년 3월~현재: 고려대학교 정보보호대학원 부교수  
관심분야: 온라인게임 보안, 네트워크 보안, 네트워크 포렌직