

헨젤과 그레텔 : 게임 내 아이템 거래를 기반으로 한 GFG 탐지 방안

이 경 민,[†] 김 휘 강[‡]
고려대학교 정보보호대학원

Hansel and Gretel : GFG Detection Scheme Based on In-Game Item Transactions

Gyung Min Lee,[†] Huy Kang Kim[‡]
Graduate School of Information Security, Korea University

요 약

MMORPG 장르의 온라인 게임은 가상현실 내의 모든 유저가 평등하다는 철학을 바탕으로 시작되었다. 모든 유저는 시간이라는 공정한 자원을 바탕으로 노력하는 만큼 대응되는 재물 혹은 지위를 얻을 수 있다. 그러나 게임 봇은 이러한 공정한 경쟁을 해치는 주된 원인으로, 선량한 게임 유저들에게 상대적 박탈감을 주어 게임에서 이탈하게 만든다. 게임 봇은 주로 GFG(Gold Farming Group)을 형성하여 활동하며, 게임 내의 재화를 무분별하게 수집하여 게임 내 경제 시스템에 악영향을 끼친다. 일반적인 게임 봇 탐지 알고리즘은 각각의 봇을 탐지하는 데에는 유용하나, 이는 GFG 전체가 아닌 일부이기에 보다 넓은 범위에서의 탐지가 필요하다. 본 연구에서는, MMORPG 장르에서 사용되는 아이템을 기반으로 GFG를 탐지하는 방안에 대해 제안한다. 게임 내에서 주로 거래되는 몇 가지 아이템들을 선정하고, 해당 아이템들의 거래 내역을 각각 네트워크로 표현하였다. GFG의 봇들이 아이템을 주고받는 특성들을 파악하고 이를 바탕으로 국내 유명 온라인 게임의 실제 데이터에서 GFG의 아이템 거래 네트워크를 식별할 수 있었다.

ABSTRACT

MMORPG genre is based on the belief that all users in virtual world are equal. All users are able to obtain the corresponding wealth or status as they strive under the same resource, time. However, game bot is the main factor for harming this fair competition, causing benign gamers to feel a relative deprivation and deviate from the game. Game bots mainly form GFG(Gold Farming Group), which collects the goods in the game indiscriminately and adversely affects the economic system of the game. A general game bot detection algorithm is useful for detecting each bot, but it only covers few portions of GFG, not the whole, so it needs a wider range of detecting method. In this paper, we propose a method of detecting GFG based on items used in MMORPG genre. Several items that are mainly traded in the game were selected and the flows of those items were represented by a network. We Identified the characteristics of exchanging items of GFG bots and can identify the GFG's item trade network with real datasets from one of the popular online games.

Keywords: Online Games, MMORPG, Game Bot, GFG, Trading Network

I. 서론

온라인 게임이 등장한 이래, 온라인 게임 시장은 지속적으로 성장해 왔으며 그 중 MMORPG는 높은 유저 점유율을 바탕으로 폭발적으로 성장해왔다. MMORPG의 주된 목표 중 하나가 게임 내 캐릭터의 성장이기에 캐릭터의 성장을 위해 필요한 게임 내 재화들의 가치는 나날이 증가하고 있다. 이로 인해 게임 내의 재화들이 현실의 재화로써 가치를 지니게 되었으며 게임사의 시스템 혹은 중개 사이트를 이용해 재화들이 현금으로 거래되기 시작하였다. 그러나 온라인 게임이 현실의 재화로써의 가치를 지니게 되자, 불법적인 방식으로 재화를 수집하여 이를 악용하는 집단인 GFG가 등장하였다. GFG는 부정한 방법을 통해 수집한 계정들을 이용하여 다량의 게임 붓을 생성하고 붓을 이용해 게임 내 재화들을 수집하여 경제적인 이익을 얻는다.

게임 붓은 별도의 조작 없이 게임 플레이를 자동으로 진행하는 프로그램으로 시간에 구애받지 않고 단순한 작업들을 반복적으로 수행할 수 있다. 게임 붓은 일반 유저와 달리 단순한 일련의 과정을 무한정 반복할 수 있기에 일반 유저에 비해 효율적이고 장기적으로 인-게임 재화를 획득할 수 있다. 이러한 게임 붓을 다수 보유하여 운용하는 단체를 GFG라 하며, GFG의 주된 목적은 인-게임 재화를 이용한 경제적인 이익의 추구에 있다.

GFG가 운용하는 게임 붓은 무차별적인 재화의 수집으로 인해 게임 내 경제시장에 악영향을 끼칠 뿐 아니라 선량한 유저들로 하여금 게임 플레이에 불편함을 느끼게 한다. 또한 MMORPG의 기본 철학인 경쟁에의 공정함을 해치고 일반 유저들에게 상대적 박탈감을 주어 게임을 이탈하도록 만드는 문제점을 지니고 있다. 온라인 게임 시장이 꾸준히 성장하기 위해서 이러한 게임 붓의 단속과 지속적인 규제는 필수불가결한 상황이기에 게임 붓 단속은 게임사에게 있어 주된 과제 중 하나이다.

현재까지, 게임사는 다양한 방법을 이용해 게임 붓을 탐지하며, 제재를 이어나가고 있다. 여러 붓 탐지 방법을 통해 다수의 게임 붓에 대한 제재가 이루어졌지만, 이는 GFG 내의 일부만을 제제한 것이기에 큰 효과를 기대하기는 어렵다. GFG는 일부 게임 붓 계정에 제재가 가해지더라도, 부정한 방법으로 수집한 다른 계정들을 이용해 손쉽게 인원을 충당할 수 있기 때문이다.

본 연구에서는 보다 넓은 범위에서의 탐지를 위해, GFG 네트워크를 판단하고 정상 유저들 사이에서 구분하는 방안을 제안한다. GFG 네트워크를 분류하기 위해 우선, 게임 내에서 주로 거래되는 아이템을 식별하고, 해당 아이템의 거래 네트워크를 추출한다. 추출한 네트워크에서, GFG 내의 붓들이 아이템을 주고받는 특성을 바탕으로 GFG의 아이템 거래 네트워크를 식별한다. 분류에 사용된 GFG 네트워크 내 아이템 거래의 특성은 다음과 같다. GFG는 다량의 게임 붓을 이용하여 게임 내의 아이템들을 수집하며 같은 계정 내의 다수의 캐릭터로부터 모은 아이템을 취합하기 위해 계정 창고 등을 이용하여 아이템을 한 캐릭터로 모으게 된다. 더 나아가, 게임 내의 경매장 시스템 혹은 유저간의 거래를 통해 해당 아이템을 판매한다.

본 연구에서는 국내 유명 온라인 게임 아이온(AION)의 실제 게임 데이터를 기반으로 게임 내 거래 네트워크를 식별하고 GFG를 분류하였다.

본 연구의 2장에서는 기존 게임 붓 탐지 방법에 대해 분석하였으며 탐지 방법론에 따라 연구들을 분류하였다. 3장에서는 게임 내의 아이템 거래를 기반으로 한 GFG 탐지 방법에 대해 제안하였으며 GFG 네트워크의 아이템 거래에 대한 특성을 파악하였다. 4장에서는 실제 게임 데이터에 제시한 방법론을 적용하여 아이템 거래 네트워크를 구성하고 GFG 내의 아이템 거래 네트워크를 식별하였다. 5장에서는 분석 결과들과 방법론의 정확도를 요약하고 결론을 기술하였다.

II. 관련 연구

게임 붓을 탐지하기 위해 많은 연구들이 이루어져 왔으며, 사용된 방법론들은 크게 클라이언트의 측면과 서버 측면으로 나눌 수 있다.

클라이언트 측면에서 사용된 방법론은 대표적으로 CAPTCHA를 이용한 챌린지-응답 방식과 게임보안 솔루션을 이용한 방식이 있다. CAPTCHA를 이용한 방식은 게임 붓과 같은 프로그램에게는 해결하기 어렵지만 사람은 해결하기 쉬운 문제를 이용해 게임 붓을 구분해내는 방식이다. 주로 게임 내에서 그림으로 이루어진 간단한 사칙연산이나 CAPTCHA 이미지를 출력하는 형태로 구현된다. 주로 사용되는 게임 보안솔루션에는 대표적으로 GameGuard, Warden, TenGuard, X-Trap 등이 있으며, 이들

Table 1. Methods for game bot detection

Category	Sub category	Methods
Client Side Detection	Challenge-response	- CAPTCHA [1][2]
	Process Monitoring	- GameGuard, Warden, TenGuard, X-Trap
Server Side Detection	User behavior analysis	- Self-similarity based analysis [3] - Route based analysis [4][5][6][7] - Action sequence based analysis [8][9] - Action frequency based analysis [10][11]
	Social network analysis	- Party based analysis [12] - Chatting pattern based analysis [13] - Trade network based analysis [14][15][16][17]

은 게임 유저의 PC에 설치되어 정보를 수집하고 불법프로그램의 실행을 제한한다. 그러나 CAPTCHA를 이용한 방식의 경우 유저의 게임 몰입도를 저해하는 단점이 있으며, 게임보안솔루션의 경우 유저의 PC에 설치된 백신 프로그램등과 충돌이 빈번히 일어나게 된다. 뿐만 아니라 봇 제작자가 게임보안솔루션을 분석하여 우회하는 방법을 찾아낼 수도 있다.

클라이언트 측면의 방법론들이 위와 같은 단점을 지니고 있기에 대다수의 게임은 서버 측면에서 게임 봇을 탐지하는 방법을 사용한다. 게임 로그를 이용하여 서버 측면에서 봇을 탐지하는 경우 탐지 방안이 봇 제작자에게 노출되지 않으며, 클라이언트 측면의 방법론에 비해 비교적 정확도가 높다는 장점이 있다. 지금까지 제안되었던 서버 측면의 탐지 방법론들은 크게 사용자의 행위 분석을 기반으로 하는 탐지 방법과 소셜 네트워크를 분석하여 봇을 탐지하는 방법으로 나눌 수 있다.

사용자의 행위 분석을 기반으로 하는 방법론에는 게임 봇의 자기 유사도를 측정하여 봇을 분류하는 방법, 게임 봇과 유저의 이동 경로를 토대로 분류하는 방법, 행동 패턴 시퀀스를 생성하여 게임 봇과 유저의 시퀀스 차이를 통해 분류하는 방법, 행동 빈도를 바탕으로 분류하는 방법 등의 연구가 진행되었다.

소셜 네트워크 분석을 통해 게임 봇을 분류하는 방법론에는 게임 내의 파티를 분석하여 봇을 탐지하는 방법, 유저의 채팅 패턴 분석을 이용하는 방법, 게임 내에서 발생하는 다양한 거래 네트워크를 분석하여 봇을 탐지하는 방법 등의 연구가 이루어졌다. 게임 봇을 탐지하는 방법론에 대한 분류는 Table 1.과 같다.

최근에는, 단순한 게임 봇 탐지를 넘어 게임 내 네트워크 분석을 통해 게임 내 재화가 현금과 같은

실제 재화로 거래되는 과정과 그 그룹들을 분석하는 연구 또한 진행되고 있다. Eunjo Lee 등은 게임 내 유저들의 플레이 스타일 등을 바탕으로 커뮤니티를 파악하고 그들의 거래 네트워크를 분석하여 더욱 넓은 범위의 GFG를 탐지하는 방안을 제안하였다 [18]. 이 외에도, 게임 내 소셜 네트워크와 거래 네트워크를 분석하여 두 네트워크의 상관관계를 파악하고 게임 내 GFG와 GFG로부터 게임 내 재화를 전달받아 유저들에게 판매하는 계정들을 판별하여 보다 넓은 범위의 GFG 네트워크를 탐지하고자 하는 연구가 진행되었다[19].

본 연구에서는 게임 내에서 주로 거래되는 아이템을 파악하고, 해당 아이템의 거래 네트워크를 구성한다. 구성된 네트워크에서, GFG의 아이템 거래 네트워크를 식별해 내어 게임 네트워크에서 GFG를 파악하고 분류할 수 있는 서버 측면에서의 탐지 방안을 제안한다.

III. 아이템 거래 기반 GFG 탐지 방안

3.1 데이터 셋 및 Ground-truth

본 연구에서는, NCSOFT 사의 MMORPG 게임인 AION의 실제 거래 로그를 바탕으로 실험을 진행하였다. 데이터 셋은 2010년 4월 9일 ~ 2010년 6월 13일까지의 게임 내 유저들의 거래 로그 및 경매장 이용 로그로, 거래 네트워크를 파악하기 위해 유저 간 거래가 아닌 상점 이용 등의 거래 로그는 제외하였다. 설정한 기간 내에 총 150만회 이상의 거래와 약 700만회의 경매장 이용이 이루어졌으며 총 9,414개의 계정이 거래를 진행하였다. 각각의 거래 로그에는 거래를 진행한 유저의 계정 정보 및 유저가

건넌 아이템의 고유 ID값이 기록되어 있으며, 이는 유저가 경매장 기능을 이용하여 아이템을 등록하고 구매할 때도 동일하다. 제안한 GFG의 거래 네트워크의 특성을 확인하기 위해 첫 44일간의 데이터를 이용하여 실험을 진행하였으며, 이후 23일간의 데이터를 통해 해당 특성이 GFG를 탐지하는 데 있어 유효함을 검증하였다.

정확한 정답지(ground-truth)를 획득하여 해당 유저가 봇인지를 판별하는 일은 GFG의 탐지에 있어서 반드시 필요한 작업이다. 정답지를 확보하기 위해 AION의 게임사인 NCSOFT에서 제공한 실제 제재 내역을 이용하였으며, 이는 게임 내의 모니터링 및 GM(Game Master)들의 결과를 바탕으로 한 제재 내역이기에 높은 신뢰도를 지니고 있다. 또한 제재의 false positive를 줄이기 위해 제재를 당한 유저가 본인의 제재에 대해 이의를 제기할 경우, 추가적인 모니터링 및 검증을 바탕으로 유저의 제재 여부를 수정하는 과정을 진행한다. 이러한 과정은 제재 내역의 신뢰도와 더불어 정확도 또한 확보할 수 있기에 본 연구에서 사용한 제재 내역은 신뢰할 만 한 정답지라고 볼 수 있다.

3.2 아이템 거래를 기반으로 한 GFG 탐지 모델

제안하는 온라인 게임의 아이템 거래를 기반으로 한 GFG의 탐지를 위한 모델은 Fig. 1.과 같다.

데이터 사전 분석 단계에서는, 전체 게임 로그로부터 유저 간 아이템 거래 내역과 경매장 이용 내역을 추출한다. 추출한 경매장 이용 내역으로부터 기간

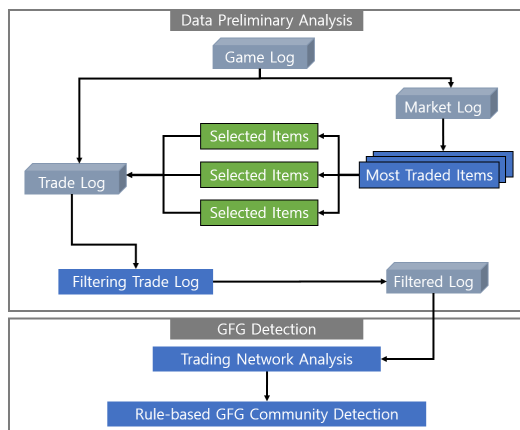


Fig. 1. Item flow based GFG detection model with data preliminary analysis

내에 가장 거래량이 많은 아이템들에 대해 GFG 탐지 목적에 알맞은 아이템들을 선별한다. 선별한 아이템에 대한 유저 간 거래 내역들을 각 아이템별로 추출하고, 유저 간 거래 내역에 대해 동일한 유저 간 기간 내 총 거래 횟수와 거래량 로그를 생성한다.

일반 유저와 GFG의 거래 네트워크를 분석하기 위해 생성한 로그를 바탕으로 아이템 별 거래 네트워크를 생성한다. 이후, 생성된 전체 거래 네트워크에서 GFG의 아이템 거래 네트워크를 분류하기 위해 GFG 거래 네트워크의 특성들을 기반으로 하여 서브네트워크들을 분류한다.

3.3 게임 내에서 주로 거래되는 아이템 정보 추출

GFG의 경우, 24시간 자동화된 사냥을 통해 재화를 수집하므로 게임 내의 아이템의 상당수를 공급한다. 이로 미루어 보아, 게임 내 전체 거래량이 높은 아이템일수록 GFG에 의한 거래량이 높을 것으로 보인다. 뿐만 아니라 해당 재화를 판매하여 유저들로부터 금전적인 이득을 취하기 위해 수요가 높은 아이템일수록 GFG에 의한 거래량이 높을 것으로 보인다. 이러한 특성을 토대로 GFG의 아이템 거래 네트워크를 식별하기 위해서는 게임 내의 전체 거래량의 상당수를 차지하는 아이템을 선정하는 과정이 필요하다. 또한 아이템의 종류에 따른 특성을 고려하여 GFG를 탐지하기 위해 분석에 이용할 아이템을 선정한다.

장비 아이템의 경우, 전체 거래량이 매우 낮은 편으로, 다수의 유저가 참여한 큰 규모의 네트워크를 표현하기에는 알맞지 않다. 또한 한 번에 거래되는 아이템의 개수가 적은 편이며, 사용하지 않는 장비 아이템을 NPC¹⁾ 등을 통해 다양한 재료 아이템으로 변경할 수 있는 아이템 분해 등의 기능을 이용해 하위 재료 아이템으로 아이템을 변경하여 거래하는 경우도 많기에 GFG 네트워크를 파악하는 데에는 적합하지 않다.

소모성 아이템과 재료 아이템의 경우, 전체 거래량의 대부분을 차지하고 있으며 해당 아이템들을 거래하는 유저 및 봇 또한 많기에 GFG 네트워크를 파악하기에 적합하다.

본 연구에서 사용하는 온라인게임인 AION 에서

1) Non Player Character의 준말. 게임 안에서 플레이어가 직접 조종할 수 없는 캐릭터로, 플레이어에게 다양한 콘텐츠를 제공하는 캐릭터를 지칭한다.

는, 소모성 아이템들이 게임 내에서 다양한 재료 아이템을 이용하여 소모성 아이템을 제작하는 조합 기능을 이용하여 제작되거나, 이벤트 및 퀘스트 보상 등을 통하여 획득되는 경우가 많다. GFG 네트워크의 봇들이 재화를 수집하는 주된 경로가 사냥 및 채집임을 감안하였을 때, 이러한 소모성 아이템들은 GFG 네트워크를 파악하기에 적합하지 않다고 판단된다. 이러한 이유로, 본 연구에서는 AION 내의 재료 아이템들의 거래를 바탕으로 GFG 네트워크를 파악하고자 한다. 거래량이 많은 아이템을 파악하기 위해, 유저들의 경매장 이용 내역을 기준으로 아이템 별 거래량을 확인한다. 전체 로그로부터, 아이템 별 경매장 등록 개수와 구매 개수가 많은 상위 아이템들을 추출하고, 아이템 종류 및 거래 개수를 정리한다.

3.4 GFG의 아이템 거래 네트워크의 특성

아이템의 거래 네트워크를 이용하여 GFG를 탐지하기 위해, 일반 유저의 거래 네트워크와 GFG의 거래 네트워크를 구분할 수 있는 특성들에 대해 파악해야 한다. 일반적인 유저의 경우, 다른 한 명의 유저와 거래하는 아이템의 총량이 비교적 적은 편이며, 불특정 다수와 거래를 진행하기에 매우 무분별한 구조의 거래 네트워크가 생성된다. GFG의 경우에는, 다수의 bot 계정을 이용하여 사냥, 채집 등의 행위를 통해 재화들을 수집하고, 최종적으로 해당 재화들을 유저들에게 판매하여 이익을 얻기 위해 소수의 계정으로 아이템을 모으는 경향이 있다. 이러한 소수의 계정을 상인(merchant)과 뱅커(banker)라고 한다[16]. Fig. 2.의 좌측 그림에서, 중심에 위치한 계정이 재화를 모으는 상인 및 뱅커이며, 이들이 속해있는 서브네트워크의 경우 Fig. 2.의 우측과 같은

구조의 네트워크가 생성된다.

IV. 실험 및 평가

4.1 GFG 네트워크의 특성 파악

GFG 네트워크의 특성을 파악하기 위해, 2010년 4월 9일 ~ 2010년 5월 20일까지의 AION 로그 데이터를 바탕으로 각 아이템 별 거래량을 추출하였으며 그중 상위 15개의 아이템에 대한 내용은 Table 2.와 같다. 해당 아이템 중 소모성 아이템은 169000008, 162000011, 141000001, 169000004, 162000006, 162000016 총 6종류로 해당 아이템들은 분석 대상에서 제외하였다.

앞서 선별한 재료 아이템들에 대한 전체 거래 네트워크를 파악하고 그 중 GFG 네트워크의 비율을 확인하기 위해 거래량이 높은 상위 9개 아이템에 대하여 각각의 전체 거래 네트워크를 생성하였으며, 생성된 네트워크 중 거래량 1위, 2위에 대한 전체 거래 네트워크는 Fig. 3.과 같다. 각 노드의 크기는 해당 노드가 건네받은 아이템의 총량에 비례하며, 간선의 굵기는 건네준 아이템의 총량에 비례한다.

전체 거래 네트워크에서 GFG 네트워크를 구별하기 위해, Fig. 2.와 같은 구조들의 네트워크가 지니는 특성을 분석하였으며, 분석한 내용을 바탕으로 설정한 GFG 네트워크의 기준은 다음과 같다.

- 1) 네트워크 내의 노드의 수가 4개 이상이다.
- 2) 최소 3개 이상의 노드로부터 아이템을 건네받

Table 2. Most traded item list between April 9 and May 20

Item id	Register	Buy
152010317	10,699,116	8,748,317
152010313	8,118,630	7,527,522
152000207	7,851,941	6,091,660
152000204	7,227,594	4,217,245
169000008	6,325,140	5,306,810
162000011	5,048,796	4,079,494
141000001	5,019,911	4,301,435
169000004	4,883,174	4,361,426
162000006	4,845,321	3,965,693
152000904	4,335,204	3,080,658
152000465	4,190,694	3,005,853
152000907	4,081,366	3,385,206
152000413	4,064,425	2,893,324
162000016	3,904,878	3,215,454
152010316	3,414,273	2,789,858

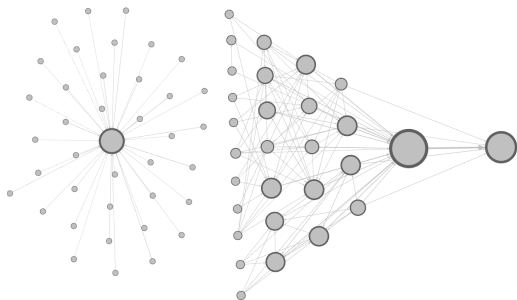


Fig. 2. GFG item distribution(left) and GFG item trade network(right)

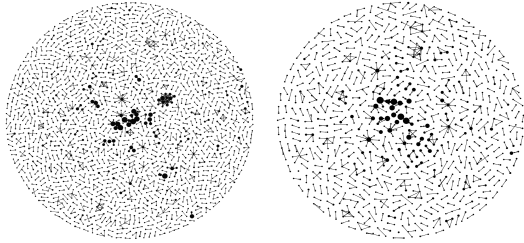


Fig. 3. Overall Trading networks of the top two most traded items

은 노드가 하나 이상 존재한다.

3) 네트워크 내의 거래 중 전체 거래량의 1% 이상의 아이템을 2)에서 확인한 노드에게 건네준 노드가 하나 이상 존재한다.

GFG의 경우, 개인 단위의 봇 사용 유저들과는 달리 기업의 형태로 구성되어 다수의 봇을 운용한다. 봇을 사용하는 개인 유저가 아닌 GFG 전체에 초점을 맞추기 위해 서브네트워크의 최소 노드 수를 4로 설정하였다. 또한 해당 노드들로부터 아이템을 집중적으로 제공받는 상인 혹은 banker 계정이 네트워크 내에 존재해야 하므로 2)와 같은 기준을 설정하였다. 마지막으로, 봇의 경우 일반 유저들에 비해 수집하는 재화의 양이 많기에 네트워크 내에 흐르는 재화의 양이 일반 유저들의 거래 네트워크에 비해 월등하다. 약 80% 이상의 유저는 타 유저에게 건네주는 아이템의 총량이 전체 거래량의 1% 미만이며, 각 아이템별 거래량 또한 같은 결과를 보였다. 이러한 분석을 토대로, 봇 유저와 일반 유저를 판별하는 최소한의 조건으로 각 아이템별 전체 거래량의 1% 이상을 거래한 적이 있는 네트워크만을 선정하였으며, 이에 대한 CDF(Cumulative Distribution Function)은 Fig. 4와 같다.

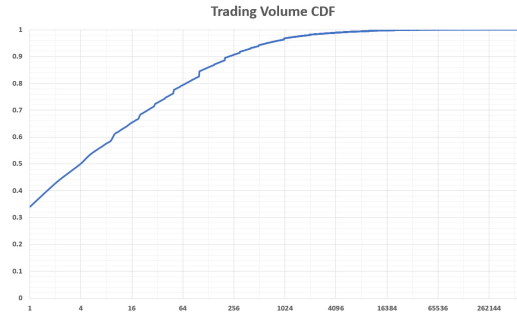


Fig. 4. CDF graph of entire trading volume

각 아이템에 대해 위의 특성을 만족하는 서브네트워크들을 추출하고, 정답지를 바탕으로 봇 유저를 판별한 결과에 대한 그림은 Fig. 5와 같으며, 초록색 노드의 경우 일반 유저를, 분홍색 노드의 경우 봇 유저를 의미한다.

선별한 아이템들에 대해, 추출한 서브네트워크에 대한 통계는 Table 3.과 같다. 총 3,935명의 일반 유저와 1,895명의 봇 유저 중 184명의 일반 유저와 1,047명의 봇 유저를 추출할 수 있었다. 9개 아이템을 이용하여 추출한 거래 네트워크에 대한 봇 탐지의 accuracy는 약 80.02%, precision은 85.05%, recall은 55.25%로, Table 4.는 탐지 결과에 대한 내용을 요약한 표이다. 해당 실험을 통해, 앞에서 언급한 GFG의 거래 네트워크의 특성이 GFG를 탐지하는 데 있어 유효함을 확인할 수 있었다.

서브네트워크 중 다수의 봇으로부터 아이템을 공급받는 일반 유저의 경우, 해당 GFG 네트워크에 포함되어있으나 봇 유저로 선별되지 않아 제재를 당하지 않은 유저로 의심해 볼 수 있다. 또한 GFG의 거래 네트워크와 유사한 구조를 지닌 일반 유저들의 거래 네트워크의 경우, 네트워크의 구조 및 거래량에서

Table 3. GFG network detection results from April 4 to May 20

Item id	Node	Edge	Avg degree	Avg weighted degree	Avg path length	Density	Clustering coefficient	Components	Accuracy
152010317	164	225	1.372	5.316	1.53	0.008	0.139	26	77.44%
152010313	120	138	1.15	3,076	1.343	0.01	0.123	20	75.83%
152000207	218	534	2.45	10,602	1.548	0.011	0.387	20	94.95%
152000204	145	213	1.469	7,539	1.751	0.01	0.152	17	82.76%
152000904	141	186	1.319	9,859	1.482	0.009	0.228	23	51.06%
152000465	121	296	2.446	25,158	1.425	0.02	0.349	15	90.08%
152000907	98	201	2.051	38,767	1.931	0.021	0.371	14	78.57%
152000413	81	151	1.864	20,312	1.656	0.023	0.274	10	88.89%
152010316	535	151	1.798	2,671	1.626	0.003	0.303	51	94.77%

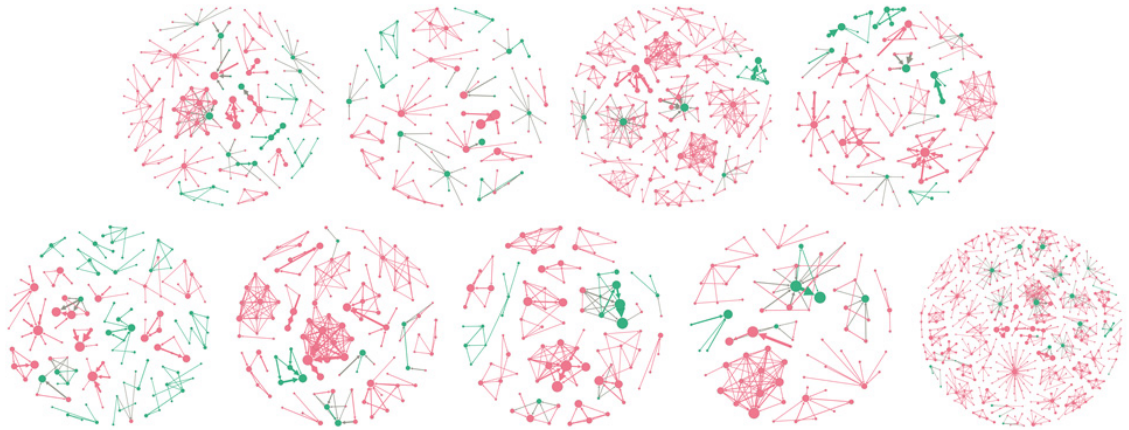


Fig. 5. Sub-networks selected by rules and GFG detection result from April 4 to May 20

Table 4. Confusion matrix of bot detection result from April 4 to May 20

	Prediction positive	Prediction negative
Condition positive	True positive 1,047	False negative 848
Condition negative	False positive 184	True negative 3,087

GFG 네트워크와의 유사성이 높기에 GFG 네트워크임을 의심해 볼 수 있다.

4.2 룰 셋 검증 및 정확도 확인

확인한 GFG 네트워크의 특성을 바탕으로, 해당 룰 셋의 적합성을 검증하기 위해 5월 21일에서 6월 13일 사이의 거래 데이터를 바탕으로 실험을 진행하였다.

이전과 마찬가지로, 거래량이 많은 상위 아이템들을 추출하였으며, 그 중 재료 아이템은 총 12개로 아이템 리스트는 Table 5.와 같다. 선별한 아이템에 대한 전체 거래 네트워크 중, GFG 네트워크의 특성을 보이는 서브네트워크들을 추출한 결과는 Fig. 6.과 같으며 이에 대한 통계는 Table 6.과 같다.

총 3,334명의 일반 유저와 898명의 봇 유저 중 90명의 일반 유저와 490명의 봇 유저를 추출할 수 있었다. 12개의 아이템을 이용하여 추출한 거래 네트워크에 대한 봇 탐지의 accuracy는 약 88.23%, precision은 84.48%, recall은 54.57%로, 이전

Table 5. Most traded ingredient item list between May 21 and June 13

Item id	Register	Buy
152010313	5,521.691	5,205,581
152010317	4,891.193	4,265,879
152000207	3,118.279	2,484,793
152000907	2,437.884	1,936,812
152000465	2,239.401	1,818,353
152000204	2,056.921	1,388,977
152000413	2,000.776	1,534,141
152000463	1,735.076	1,239,491
152000415	1,558.571	1,298,837
152010316	1,538.037	1,155,908
152000904	1,438.069	1,040,701
152010312	976.504	808,733

실험과 비슷한 성능을 보였으며 Table 7.은 탐지 결과에 대한 내용을 요약한 표를 나타낸다. 두 번의 실험에서, accuracy와 precision은 약 85%의 성능을 보인 반면, recall은 약 55%의 수치를 나타내었다. 정상 유저로 판단되었으나 봇으로 의심되는 유저들을 고려하였을 때, 해당 룰 셋의 accuracy와 precision은 봇과 의심 유저를 탐지하는 데 적합한 성능을 보이고 있다고 이야기할 수 있다. 그러나 recall 수치로 미루어 보아, 해당 룰 셋이 게임 내 모든 봇 유저를 탐지하지는 못함을 알 수 있다.

152000465의 ID를 가진 아이템과 같은 일부 아이템들은, 총 두 차례의 시험동안 정확도의 변동이 매우 큰 편이었으며, 정확도가 매우 낮은 현상을 보였다. 그러나 관측 기간을 4월 9일부터 6월 13일까지로 늘려 이를 관측한 결과, 152000465의 경우

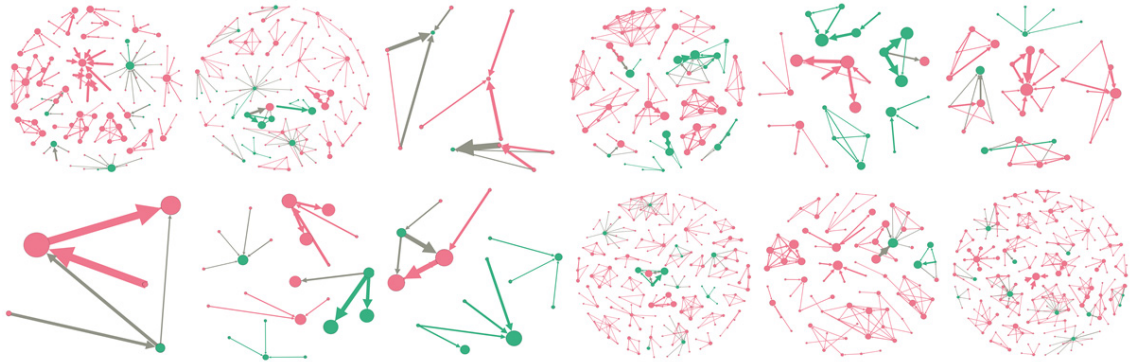


Fig. 6. Sub-networks selected by rules and GFG detection result from May 21 to June 13

Table 6. GFG network detection results from May 21 to June 13

Item id	Node	Edge	Avg degree	Avg weighted degree	Avg path length	Density	Clustering coefficient	Compo-nents	Accuracy
152010313	126	148	1.175	1349	1.483	0.009	0.124	19	92.06%
152010317	141	173	1.227	5019	1.249	0.009	0.158	23	84.40%
152000207	13	14	1.077	7238	1.278	0.09	0.205	3	84.62%
152000907	93	217	2.333	28576	1.487	0.025	0.453	14	77.42%
152000465	30	37	1.233	21785	1.302	0.043	0.247	7	53.33%
152000204	36	51	1.417	4358	1.19	0.04	0.342	6	77.78%
152000413	5	6	1.2	53819	1.333	0.3	0.2	1	80.00%
152000463	22	22	1	26897	1.353	0.048	0	5	63.64%
152000415	14	13	0.929	24501	1.188	0.071	0.071	3	71.43%
152010316	197	309	1.569	2290	1.539	0.008	0.302	30	92.39%
152000904	81	137	1.691	9762	1.646	0.021	0.23	12	95.06%
152010312	214	335	1.565	1864	1.676	0.007	0.312	29	94.86%

87.15%의 정확도를, 152000904의 경우 83.8%의 정확도를 보여주었으며 이외의 아이템들도 평균적으로 약 85%의 정확도를 보여주었다. 가장 낮은 정확도를 보여주었던 두 아이템에 대한 전체 기간의 네트워크 그림은 Fig. 7.과 같다. 해당 결과를 통해, GFG 탐지에 있어 충분한 양의 데이터를 수집할 수 있다면 탐지에의 정확도를 보장할 수 있음을 알 수 있다.

결과적으로, 본 연구의 GFG 탐지 모델은 봇 탐

지에 있어서는 약 85%의 accuracy 및 precision을 보여주었으며, 일반 유저라고 판별된 유저들의 대다수는 GFG의 거래 네트워크 내에 위치해 있거나 GFG의 거래 네트워크와 유사한 형태의 네트워크를 형성하고 있었기에 GFG에 속해있는 유저라고 의심해 볼 수 있다. 이러한 점으로 미루어보아, 본 연구

Table 7. Confusion matrix of bot detection result from May21 to June 13

	Prediction positive	Prediction negative
Condition positive	True positive 490	False negative 408
Condition negative	False positive 90	True negative 3,244

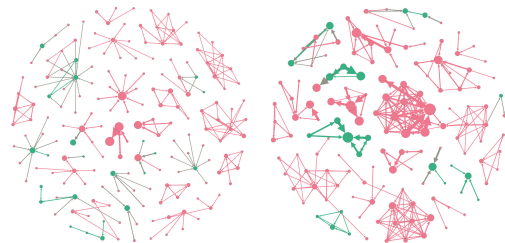


Fig. 7. Sub-networks selected by rules and GFG detection result of 152000465(left) and 152000904(right) from April 9 to June 13

에서 제안하는 탐지 모델은 봇 유저뿐 아니라, 기업에서 주로 모니터링 해야 할 봇 의심 유저 또한 함께 추출할 수 있을 것으로 보인다. 또한 사용한 로그들과 피쳐들은 대부분의 온라인 게임에서 추출할 수 있는 정보들이기 때문에 다른 온라인 게임에도 본 연구의 모델을 적용할 수 있을 것으로 기대된다.

V. 결 론

본 논문은 게임 내 아이템 거래 네트워크를 바탕으로 GFG 네트워크를 확인하는 첫 번째 시도로, 온라인 게임에서의 아이템 거래 네트워크를 파악하고 GFG의 거래 네트워크가 지니는 특성을 분석하여 봇 유저와 함께 봇 의심 유저군 또한 탐지해 낼 수 있는 아이템 기반 GFG 네트워크 탐지 모델을 제안하였다.

국내 유명 온라인 게임인 AION의 거래 데이터를 통하여 GFG 네트워크가 가질 수 있는 특성들을 확인하였고, 제안한 탐지 방안에 적용하여 봇 탐지에의 약 85%의 accuracy 및 precision을 보였다. 제재 내역에 기반 하여 봇이 아니라고 판단된 유저들의 경우, 속해있는 네트워크의 분석 및 네트워크 구조 등을 토대로 봇 유저임에도 불구하고 게임 내에서 봇으로 탐지되지 않은 유저로 판단된다. 그러나 데이터의 한계로 인해, 해당 탐지에 대한 추가적인 확인을 할 수 없어 보다 면밀한 검증이 불가능 한 점은 아쉬운 부분이다.

기존의 봇 탐지 연구는 온라인 게임 내의 단일 봇을 탐지하는 데에 초점이 맞추어져 있었으나, 본 논문에서 제안한 GFG 네트워크 탐지 방안은 GFG 네트워크 내의 단일 봇이 아닌 GFG 네트워크 전체를 파악할 수 있다. GFG 네트워크 탐지를 통해 게임 내에 존재하는 다수의 게임 봇에 대한 제재 및 관리가 이루어질 수 있으며 게임 내의 재화 유통의 상당 부분을 도맡고 있는 GFG 네트워크에 대한 제재 및 관리 또한 이루어질 수 있다. 더 나아가, 봇으로 탐지되지 않았으나 GFG와 긴밀한 관계를 맺고 있는 유저, GFG 네트워크로 의심할 수 있는 거래 네트워크 등을 함께 확인할 수 있어 보다 넓은 범위의 봇 탐지가 가능하다.

향후, 본 연구에서 제안한 방안에 대해 다른 데이터를 이용하여 해당 방안의 범용성을 검증할 예정이며, GFG 네트워크의 특성 또한 추가함으로써 보다 높은 정확도를 보이도록 모델을 개선할 계획이다.

References

- [1] Philippe Golle and Nicolas Ducheneaut, "Preventing bots from playing online games," *Computers in Entertainment (CIE)*, vol. 3, no. 3, pp. 3-3, July 2005.
- [2] Yampolskiy, Roman V., and Venu Govindaraju, "Embedded noninteractive continuous bot detection," *Computers in Entertainment (CIE)*, vol. 5, no. 4, pp. 7-7, Aug. 2007.
- [3] Eunjo Lee, Jiyoung Woo, Hyoungshick Kim, Aziz Mohaisen, and Huy Kang Kim, "You are a game bot!: uncovering game bots in MMORPGs via self-similarity in the wild," *NDSS*, Feb. 2016.
- [4] Kuan-Ta Chen, Andrew Liao, Hsing-Kuo Kenneth Pao, and Hao-Hua Chu, "Game bot detection based on avatar trajectory," *Proceedings of the 7th International Conference on Entertainment Computing*, pp. 94-105, Sept. 2008.
- [5] Mitterhofer Stefan, Platzler 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.
- [6] van Kesteren, Marlieke, Jurriaan Langevoort, and Franc Grootjen, "A step in the right direction: bot detection in MMORPGs using movement analysis," *Proc. of the 21st Belgian-Dutch Conference on Artificial Intelligence*, pp. 129-136, 2009.
- [7] Chen, Kuan-Ta, Hsing-Kuo Kenneth Pao, and Hong-Chung Chang, "Game bot identification based on manifold learning," *Proceedings of the 7th ACM SIGCOMM Workshop on Network and System Support for Games*. ACM, pp.

- 21-26, Oct. 2008.
- [8] 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.
- [9] 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.
- [10] 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.
- [11] Ruck Thawonmas, Yoshitaka Kashi-fujik, 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.
- [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] 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.
- [14] 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.
- [15] 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.
- [16] Hyukmin Kwon, Aziz Mohaisen, Jiyoung Woo, Yongdae Kim, Eunjo Lee, and Huy Kang Kim, "Crime scene reconstruction: online gold farming network analysis," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 544-556, Mar. 2017.
- [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] Eunjo Lee, Jiyoung Woo, Hyoungshick Kim, and Huy Kang Kim, "No silk road for online gamers!: using social network analysis to unveil black markets in online games," *WWW '18 Proceedings of the 2018 World Wide Web Conference*, pp. 1825-1834, April. 2018.
- [19] Selin Chun, Deajin Choi, Jinyoung Han, Huy Kang Kim, and Taekyoung Kwon, "Unveiling a socio-economic system in a virtual world: a case study of an MMORPG," *WWW '18 Proceedings of the 2018 World Wide Web Conference*, pp. 1929-1938, April. 2018.

 <저자소개>



이 경 민 (Gyung Min Lee) 학생회원
 2018년 2월: 고려대학교 컴퓨터학과 졸업
 2018년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
 <관심분야> 정보보호, 온라인게임 보안, 시스템 보안



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~20104년 12월: 고려대학교 정보보호대학원 조교수
 2015년 1월~현재: 고려대학교 정보보호대학원 부교수
 <관심분야> 온라인게임 보안, 네트워크 보안, 네트워크 포렌식