Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.5, Oct. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.5.1097

온라인 게임에서의 이상 징후 탐지 기법 조사 및 분류*

곽 병 일,† 김 휘 강‡
고려대학교 정보보호대학원

A survey and categorization of anomaly detection in online games*

Byung Il Kwak,† Huy Kang Kim‡
Graduate School of Information Security, Korea University

요 약

빠르게 성장한 게임 시장의 규모에 따라 게임봇, 게임핵, 골드파밍, 사설서버, 시스템 해킹, 네트워크 해킹, 계정 도용 등과 같은 게임을 이용한 여러 불법 행위가 증가해 왔다. 이러한 불법 행위를 예방 및 탐지하기 위해 게임 보안 솔루션들이 존재하지만 각 게임마다의 특징이 존재하기 때문에 부정행위로부터 보호하는 것에는 어려움이 있다. 또한 게임 보안은 게임의 기획과 조화되는 게임 보안 솔루션 및 탐지 방법들이 필요하다. 본 연구에서는 최근 온라인 게임에서의 보안 관련 연구에 대한 동향을 조사하였다. 온라인 게임에서의 부정행위를 분류하였고, 온라인 게임에서의 각 특징에 따른 부정행위 예방 및 탐지 방법을 분류하였다.

ABSTRACT

As the online game market grows, illegal activities such as cheating play using game bots or game hack programs, running private servers, hacking game companies' system and network, and account theft are also increasing. There are various security measures for online games to prevent illegal activities. However, the current security measures are not enough to prevent all highly evolving game attacks and frauds. Some security measure can do harm game players usability, game companies need to develop usable security measure that is well fit to game genre and contents design.

In this study, we surveyed the recent trend of various security measure applied in online games. This research also classified illegal activities and their related countermeasure for detection and prevention.

Keywords: survey, categorization, taxonomy, online game, detection

I. 서 론

국내 및 국외 게임 시장은 지금까지 빠르게 증가해 왔다. 글로벌 리서치 기업 뉴주(Newzoo)는 2014년 세계 게임 시장이 750억 달러에 달하는 것을 밝혔다. 각 국가별 게임 시장 규모에서 미국은 20,485백만 달러에 달했고, 그 뒤를 이어 중국은 17,867백만 달러, 일본은 12,220 백만 달러에 달했다. 독일은 3,528백만 달러, 영국은 3,426 백만 달러에 달하고 그 뒤로 한국이 6위인 3,356 백만 달러에 달한다고 밝혔다[1].

Fig.1.은 게임 시장에서 플랫폼 별 시장의 분포를 나타낸 것이다. 콘솔 게임 플랫폼의 경우 미국에서 약 51%, 일본에서 약 39%, 독일에서 약 48%, 영국에서 약 51%로 가장 높은 비율을 차지하는 것으로 나타났다. 반면 중국과 한국의 경우 온라인 게임

접수일(2015년 6월 24일), 수정일(2015년 8월 31일), 게재확정일(2015년 9월 23일)
* 본 연구는 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (과제번호 :2014R1A1A1006228)
추가로 본 연구는 고려대학교 특별연구비에 의하여 수행되었음
† 주저자, kwacka12@korea.ac.kr
‡ 교신저자, cenda@korea.ac.kr(Corresponding author)

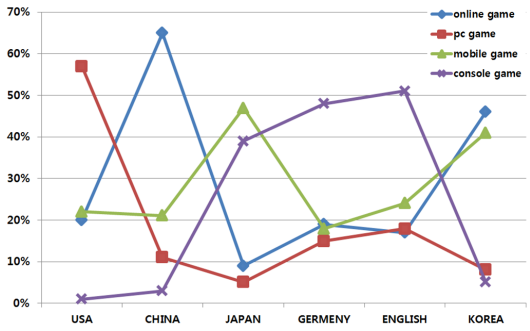


Fig. 1. 2014 National Game Market

플랫폼이 높은 비율을 차지하는 것으로 나타났다[1].

게임 시장의 규모가 성장함에 따라 게임을 이용한 여러 불법 행위 또한 증가하고 있다. Ahnlab은 온라인 게임핵 악성코드가 전체 악성코드 탐지 순위에서 6위인 것으로 밝혔다[2].

게임 내에서 이루어지는 부정행위에는 게임봇, 게임핵, 골드파밍, 사설서버, 시스템 해킹, 네트워크 해킹, 계정도용 등이 있다. 이 중 많이 사용되고 있는 부정행위는 게임봇을 이용한 자동 플레이 프로그램의 사용이다. 게임봇은 사용자 본인이 게임 플레이를 하는 것이 아닌 사용자가 지정해둔 명령을 프로그램이 자동적으로 수행하여 게임 캐릭터의 레벨 및 게임 재화를 쉽게 얻을 수 있는 프로그램이다. 게임봇은 개인 플레이어가 게임을 보다 쉽게 플레이하기 위해 사용할 뿐만 아니라 전문적으로 돈을 벌기 위해 작업장을 운영해 대규모로 이용하고 있다.

게임 내 부정행위를 막기 위해 게임 업체의 경우 안티 치팅 솔루션을 적용하고 있다. 국내의 경우 nProtect, Hackshield, DexGuard 등과 같은 게임 보안 솔루션을 전문적으로 상용한 제품이 있고, 국외의 경우 iOvation, Kount, Warden 등의 안티 치팅 솔루션을 적용하고 있다. 게임 보안 솔루션들은 게임의 악성코드, 게임핵, 메모리 조작, 메모리 해킹 등과 같은 공격들의 실행을 막아 부정행위를 방지하는 기능을 한다. 하지만 이러한 제품으로도 게임 내 부정행위를 완벽하게 막는 것에는 어려움이 있다. 그 이유로는 게임의 특성에 맞춘 게임 보안 솔루션에 있다. 게임의 장르마다 게임에 적용되는 부정행위의 종류가 다르기 때문에 이를 막기 위한 보안 솔루션 역시 다양한 방식으로 적용이 되어야 한다. 또한 게임 기획과 함께 조화가 가능한 보안 솔루션의 적용되어야 한다.

본 연구에서는 온라인 게임에서 행해지는 부정행위들을 살펴보았다. 또한 부정행위를 효과적으로 탐지할 수 있는 방법들을 다양한 기준으로 분류하였다. 게임마다 적용 가능한 특징들이 있기 때문에 게임 특성에 맞는 부정행위 탐지 방법들을 살펴보았다. 본 논문은 2장에서 이전 게임 내 이상 징후 탐지 방안들에 대한 참고문헌을 살펴보고, 3장에서는 온라인 게임 내에서 일어날 수 있는 부정행위를 살펴본다. 4장에서는 온라인 게임에서의 이상 징후 탐지를 여러 관점에서 분류하고 5장 설명을 끝으로 마무리한다.

II. 문헌 연구

Jeff Yan 등은 온라인 게임에서 발생 가능한 보안적인 실패의 요인과 서비스 제공업체에서 고려해야 할 이슈에 대해 나타내었다. 온라인 게임에서의 다양한 치팅 행위와 이를 예방 및 완화시키는 방안들을 제시하였다[3].

Jeff Yan은 온라인 게임에서 부정행위 탐지 및 완화에서 컴퓨터 게임 그래픽과 AI의 중요성을 온라인 게임의 시스템 디자인 및 유저 인터페이스 디자인을 통해 나타내었다. 또한 게임 내 공정성을 강화하기 위해 서버에서 민감 데이터 유지, 부정행위 방지를 위해 시스템적인 디자인 설계, 침입 탐지를 위한 네트워크 및 호스트 기반의 IDS 사용, 평판 관리 시스템을 통해 제시하였다[4].

Jiyoung Woo 등은 온라인 게임에서 발생하고 있는 부정행위를 분류 및 정의 하였고, 온라인 게임에서의 위협 및 부정행위에 대한 대응방안들을 클라이언트 단, 네트워크 단, 서버 단으로 분류하여 정리하였다. 과거에 연구되었던 게임봇 탐지 및 계정 도용 탐지에 대한 방법론들을 클라이언트 단, 네트워크 단, 서버 단 3가지 카테고리에 맞춰 나타내었다[5].

III. 온라인 게임에서의 부정행위

게임에서의 부정행위는 부정 사용자에게 게임 재화나 편의성을 제공하지만 게임 회사 및 일반 사용자에게는 직간접적인 피해를 준다. 온라인 게임 부정행위로 인한 피해는 크게 두 가지로 나눌 수 있다. 첫째, 부정 사용자는 유료 아이템을 무료로 사용하거나 게임봇을 이용하여 시간의 소비 없이 재화를 획득할 수 있어 게임 회사에게 금전적 피해를 준다. 둘째, 부정 사용자의 부정행위로 일반 사용자는 게임에서의

Table 1. Illegal act in online games

Category	Description
Game bot	- An automated program instead of user's gameplay - Categorized by hardware type and software type depending on physical form
Game hack	- A program to get profit through manipulation of memory and network traffic
Gold farming	- Illegal activity to get profit through inexpensive labor - Categorized by play human type and game bot type depending on conduct
Private server	- Service server of duplication without allow of game company - Categorized by server of engineering analysis and server of duplication source code depending on creating
System hacking and network hacking	- A remote attack of aiming at game server - At the attack success, modification history of user's item data
Account steal	- Hijacking user's information in game client side through malware

게임 내 재화 불균형과 상대적 박탈감을 느끼게 되어 게임에 대한 신뢰를 잃고 게임에서 이탈하거나 피해를 보상받기 위해 부정 사용자가 된다. 부정행위를 도와주는 툴은 인터넷 카페나 블로그 등을 통해 유포되고 누구나 쉽게 접근할 수 있다. 또한 부정행위 도구는 조작 방법이 어렵지 않아 일반인도 손쉽게 사용할 수 있어 문제가 있다.

Table 1.은 온라인 게임에서 발생하는 부정행위를 나타낸 것이다. 온라인 게임에는 게임봇, 게임핵, 골드파밍, 사설 서버, 시스템 및 네트워크 해킹, 계정 도용 등과 같은 다양한 부정행위가 있다.

게임봇은 유저 대신 게임을 플레이하는 자동화된 프로그램으로 하드웨어 방식과 소프트웨어 방식으로 분류할 수 있다. 하드웨어 방식은 USB 및 자동 매크로 기능이 있는 기기를 PC에 연결하여 사용하는 방식이다. 소프트웨어 방식은 PC에 별도의 프로그램을 설치하여 실행하는 방식이다. 게임봇은 동작방식으로 분류하면 IG (in game client) 봇과 OOG (out of game client) 봇이 있다. IG 봇은 게임 클라이언트 안에 서 수행하는 게임봇으로 후킹 방식에 따라 클라이언트 단 및 서버 단에서 탐지하기 어려운 특징이 있다. OOG 봇은 게임의 구조 및 분석이 모두 끝났을 경우 발생되고, 서비스 기간이 길고 보안이 전혀 고려되지 않은 게임에 발생한다.

게임핵은 사용자의 플레이 방식을 임의로 변경하여 부정행위를 일으키는 프로그램으로 게임 클라이언트의 메모리 조작 또는 네트워크 트래픽 조작을 통해 발생한다. 일반적으로 FPS (first-person shooter)게임에서는 게임의 속도를 향상 시키는 스피드 핵(speed hack), 적편의 대상을 마주쳤을 경우 총의 반동을 없애주는 무반동 핵, 벽과 같은 장애물을 투시하여 다른 사용자를 보여주는 월 핵(wall hack) 등이 있고 그 외에도 무기 핵, HP 핵, 경험치 핵, 관통 핵, 맵 핵 등 많은 종류의 게임핵이 존재한다.

골드파밍은 값싼 노동력을 이용해 게임 내 재화를 습득하는 부정행위로 게임봇을 이용하는 방식과 사람이 직접 게임 플레이하는 방식이 있다. 사람이 직접 게임 플레이하는 경우 이를 탐지하는 것이 어렵지만 사람이 운영 가능한 캐릭터 개수 제한의 단점이 있다. 게임봇을 이용하는 방식은 여러 대의 컴퓨터에 게임봇을 설치하여 동시에 운영하기 때문에 사람은 관리를 통해 골드파밍을 수행한다. 게임봇 프로그램은 설정된 행동만 수행하기 때문에 비교적 쉽게 탐지가 가능하다.

사설 서버는 서비스 중인 게임 서버를 복제하여 게임 업체의 동의 없이 서비스하는 서버를 말한다. 사설 서버는 역공학 분석을 이용하여 구성한 사설 서버와 원래의 소스 코드를 복제하여 구성한 사설 서버로 나눌 수 있다. 역공학 분석을 이용한 사설 서버는 기존 게임의 클라이언트 분석과 네트워크 트래픽 분석을 통해서 서버를 재구성한다. 소스 코드를 복제하여 생성한 사설 서버는 기존 서버를 완벽하게 복제한 것이기 때문에 일반 게임 서버와 차이점이 적은 특징이 있다.

시스템 및 네트워크 해킹은 게임 서버를 대상으로 원격 공격을 수행하는 부정행위이다. 시스템 및 네트워크 해킹은 주로 공격에 성공하면 게임 DB안의 데이터를 변조 하거나 게임 소스 복사를 목적으로 한다. 시스템 및 네트워크 해킹의 공격으로는 DDoS

Table 2. Research classification of online game security

Category	Detailed category	
Detection side	- Client side : anomaly detection of user behavior in game client side - Network side : anomaly detection of playing the online game at a network side - Server side : anomaly detection of character behavior in server side	
Detection technique	- Statistics - Data mining	- Similarity analysis - Turing test
Detection algorithm	- Decision Tree - Support Vector Machine - Random Forest - Neural Network	- Hidden Markov Model - Bayesian Network - CAPTCHA - Entropy analysis
Data source	- Character behavior - Character travel path - User behavior	- Social network - Network traffic - Image source
Game genre	- Massive Multiplayer Online Role Playing Game (MMORPG) - First-Person Shooter (FPS) - Card Game	- Racing Game
Detection target	- Game bot detection - Account steal detection - Gold farming group detection	- Game hack detection - Game bot prevention

공격, 패킷/응답 공격, 웹 사이트 취약점 해킹과 같은 일반적인 인터넷 및 네트워크 공격에 해당하는 공격들이 있다.

계정 도용은 게임을 이용하는 사용자의 계정을 탈취하는 것으로 클라이언트 단에 악성코드를 설치 후 개인의 정보를 수집하여 사용자 계정을 탈취한다. 탈취된 계정의 경우 계정 내 자산인 아이템 및 게임 재화를 잃게 된다.

IV. 온라인 게임에서의 이상 징후 탐지 및 보안

온라인 게임에서는 다양한 부정행위 및 이상 징후 발생이 가능하다. 이상 징후에 대한 보안조치는 게임의 특징 및 환경에 따라 다르게 적용 되어야 한다. Table 2.는 온라인 게임에서의 이상 징후 탐지 및 대응에 대한 연구들을 다양한 관점에서 분류한 것이다. 연구에 대한 분류 기준은 탐지 단, 탐지 기법, 탐지 알고리즘, 데이터 소스, 게임 장르, 탐지 대상과 같다.

4.1 탐지 단에 따른 분류

이상 징후 탐지의 경우 탐지 위치에 따라 분류가 가능하다. 이상 징후를 탐지하는 위치는 크게 세 부분으로 서버 단, 네트워크 단, 클라이언트 단으로 나눌 수 있다. Table 3.은 온라인 게임 관련 보안 연구들을 서버 단, 네트워크 단, 클라이언트 단에 맞춰 분류한 것이다.

서버 단에서의 이상 징후 탐지는 유저들이 온라인 게임을 플레이할 경우 플레이 로그들이 서버에 저장되는데 이 로그의 분석을 통해서 이상 징후 발생 여부를 탐지한다. Yutaro Mishima 등은 게임 플레이 로그에 대한 캐릭터 행위 빈도 및 속도를 분석하여 특징으로 추출하고, 통계적 기법에 적용하여 MMORPG에서 게임봇과 일반 사용자를 분류하였다[6]. Atsushi Fujita 등은 서버 단에서 유저들의 거래 네트워크를 데이터 마이닝 기법에 적용하여 RMT (Real Money Trade) 탐지 방법을 제시하였다. RMT는 게임 재화를 현금으로 환전하는 거래를 의미한다. RMT의 경우 탈세, 돈세탁 등과 같은 현실에서 지하경제의 부정 거래를 이용하는데 사용된다. 제시한 방법론은 유저들 사이의 거래 네트워크에서 거래 횟수, 거래 머니의 양 및 현재 보유중인 게임 머니의 양을 특징으로 추출하고, SVM 알고리즘에 적용하여 MMORPG에서 RMT를 탐지하였다[7]. Muhammad Aurangzeb Ahmad 등은 서버 단에서 사용자들의 현금거래 네트워크 및 행위를 데이터 마이닝 기법에 적용하여 골드파밍 탐지 방법을 제시하였다. 제시한 방법론은 사용자와 골드파머들의 거래 횟수 및 한 번에 이뤄지는 거래 량, 거래

Table 3. Classification depending on a detection side

Category	Research	Characteristic	Key research
Server side	[6-42]	- Performing through the game log analysis of user behavior - Control a restriction time and scale - Bypass of detection by leak of detection rule	- “User identification based on game-play activity patterns” [9]
Network side	[43-45]	- Guarantee of game performance - Increasing computation power of encryption and decryption in traffic data	- “Identifying MMORPG bots: A traffic analysis approach” [43]
Client side	[46-48]	- Collecting of detection information in PC - Falling of game usability, and easy bypass of detection	- “Identification of Auto Programs by Using Decision Tree Learning for MMORPG” [46]

물품의 종류와 같은 특징을 추출하고, Naive Bayes, Bayes Network, Logistic Regression, KNN, J48, AdaBoost 와 같은 다양한 알고리즘에 적용하여 MMOG에서 골드파머를 분류하였다[8]. Kuan-Ta Chen 등은 서버 단에서 캐릭터의 게임 내 활동 시간과 유휴 시간을 특징으로 추출하고, 이들에 대한 분포 및 엔트로피 비교를 통해 MMORPG에서 게임봇을 탐지하였다[9].

네트워크 단에서의 이상 징후 탐지는 온라인 게임을 이용할 경우 게임 클라이언트 프로그램과 서버와의 네트워크 통신 트래픽이 발생하는데 이 트래픽 분석을 통해서 이상 징후 발생 여부를 확인한다. Chen Kuan Ta 등은 네트워크 단에서 전송 트래픽의 규칙성 및 폭발성을 분석하여 특징으로 추출하고, 통계적 기법에 적용하여 MMORPG에서 게임봇을 분류하였다[43]. Sylvain Hilaire 등은 네트워크 단에서 네트워크 트래픽 데이터를 데이터 마이닝 기법에 적용하여 게임봇 탐지 방법을 제시하였다. 제시한 방법론은 서버와 클라이언트간의 전송되는 패킷의 시간 간격과 패킷의 사이즈를 특징으로 추출하고, Decision Tree 알고리즘에 적용하여 MMORPG에서 게임봇을 탐지하였다[44].

클라이언트 단에서의 이상 징후 탐지는 게임 클라이언트가 설치되어 있는 사용자 PC가 악성코드에 감염되어 위협에 노출된 경우에 탐지하는 부분이다. Sungwoo Hong 등은 클라이언트 단에서 사용자 행위를 데이터 마이닝 기법에 적용하여 게임봇 탐지 방법을 제시하였다. 제시한 방법론은 사용자의 키보드 및 마우스 입력 시퀀스를 포함한 윈도우 이벤트 시퀀스를 특징으로 추출하고, Decision Tree 알고리즘에 적용하여 MMORPG에서 게임봇을 탐지하였다[46].

4.2 탐지 기법에 따른 분류

이상 징후 탐지의 경우 탐지 기법에 따라 분류가 가능하다. 이상 징후 탐지 기법은 데이터 마이닝 기법, 통계적 기법, 유사도 패턴 매칭 기법, 튜링 테스트 기법으로 나눌 수 있다. Table 4.는 데이터 마이닝 기법, 통계적 기법, 유사도 패턴 매칭 기법, 튜링 테스트 기법에 따른 온라인 게임 관련 보안 연구들을 분류한 것이다.

데이터 마이닝 기법은 게임 상에서 캐릭터의 행위 및 유저들의 행위들을 분석하여 데이터들 간의 유용한 상관관계 발견 및 유의미한 정보를 추출하여 의사결정에 사용하는 기법이다. Jina Lee 등은 서버 단에서 캐릭터의 행위 시퀀스를 데이터 마이닝 기법에 적용하여 게임봇을 분류하였다. 제시한 방법론은 게임 내 캐릭터의 행위 시퀀스를 특징으로 추출하고, Naive Bayesian 알고리즘에 적용하여 MMORPG에서 게임봇을 분류하였다[12]. Su-Yang Yu 등은 서버 단에서 캐릭터의 행위를 데이터 마이닝 기법에 적용하여 Aim 봇 분류방법을 제시하였다. 제시한 방법론은 적의 타겟을 조준하는데 걸리는 가속도와 조준을 유지하는 시간과 같은 특징을 추출하고, SVM 알고리즘에 적용하여 FPS에서 Aim 봇을 분류하였다[13].

통계적 기법은 게임 내 일반 유저와 부정행위자들의 로그 데이터를 특정 지어 분산, 평균, 표준 편차 및 분포와 p-value, z-value 등을 통해 유저와 부정행위자를 구분하는 기법이다. Marlieke van Kesteren 등은 클라이언트 단에서 게임 내 캐릭터의 움직이는 각도에 따른 빈도를 특징으로 추출하고, 통계적기법에 적용하여 MMORPG에서 게임봇을 탐지하였다[48]. Jehwan Oh 등은 서버 단에서 캐릭

Table 4. Classification depending on a detection technique

Category	Research	Characteristic	Key research
Data mining	[7-8],[12-13],[18-26],[27-29],[32-34],[36-37],[42],[44-46]	- High accuracy of anomaly detection - Limitation of application in real-time and client side because of using much time of data analysis	- "Aimbot detection in online fps games using a heuristic method based on distribution comparison matrix" [23]
Statistics	[6],[9],[10],[14-16],[24],[30-31],[38-39],[41],[43],[48]	- Limitation of application in new character because of requiring data accumulation - Requiring lots of data to create detection rule	- "Automatic detection of compromised accounts in mmorpgs" [14]
Similarity analysis	[11],[17],[40]	- Limitation of application in new character because of requiring data accumulation - Limitation of application in client side because of increasing computation quantities	- "Server-side bot detection in massive multiplayer online games" [11]
Turing test	[23],[35],[47]	- Applicable to the real time because of a little computation - Applicable to the precautionary step - Falling of game immersion	- "Development of embedded CAPTCHA elements for bot prevention in fischer random chess" [23]

터의 경험치, 거래, 로그인 데이터와 같은 특징을 추출하고, 통계적 기법에 적용하여 MMORPG에서 계정 도용을 탐지하였다[14].

유사도 분석 기법은 일반 유저와 게임봇의 행위 분석 시 현재와 이전 행위간의 유사성 분석을 통해 게임봇을 분류하는 기법이다. 게임봇의 경우 사전에 입력된 행위만을 반복하기 때문에 유사도 패턴이 유사하게 나타나지만 일반 유저의 경우 사냥 외에 채집, 채팅, 거래, 파티, 길드 활동 등 다양한 행위를 수행하기 때문에 유사도 분석 시 다르게 유사도가 나타난다. Stefan Mitterhoffer 등은 서버 단에서 게임 캐릭터의 이동 패턴을 유사도 패턴 매칭 기법에 적용하여 게임봇 분류 방법을 제시하였다. Waypoint는 게임내 캐릭터의 이동 기점을 말하는 것으로 게임 유저들의 이동 경로 중 가장 높은 빈도로 머무는 장소를 의미한다. 제시한 방법론은 게임 유저들의 이동 경로 중 가장 높은 빈도로 머무는 장소인 Waypoint를 추출하였다. 추출된 Waypoint 정보를 LCP (Longest Common Prefix) 알고리즘에 적용하여 MMOG에서 게임봇을 분류하였다[11]. LCP는 두 단어 및 문장이 있을 경우 접미사의 최대 공통 접두사의 길이를 의미하며 일반적으로 문자열 비교를 수행 시 사용되는 알고리즘이다. Christian Platzer는 서버 단에서 캐릭터의 행위 시퀀스를 유사도 패턴 매칭 기법에 적용하여 게임봇 탐지 방법을 제시하였다. 제시한 방법론은 캐릭터의 전투 행위를 시퀀스로 나타내어 시퀀스들간의 거리를 추출하고, Levenshtein distance 알고리즘에 적용하여 MMOG에서 게임봇을 탐지하였다[17]. Levenshtein distance 알고리즘은 두 개의 문자열을 비교할 때 한 문자열이 다른 문자열로 바뀌기 위해서 필요한 변경 횟수를 측정하는 알고리즘으로 두 개 문자열의 유사성을 측정하는데 사용된다.

튜링 테스트 기법은 기계는 인지하고 판별하는 것이 어렵지만 사람은 쉽게 인지하여 판별할 수 있게 하여 기계와 사람을 분류하는 기법이다. Ryan McDaniel 등은 서버 단에서 이미지에 대한 특징을 튜링테스트에 적용하여 체스 게임에서 게임봇 사용을 예방하는 방법을 제시하였다. 제시한 방법은 이미지 회전, 이미지 해상도 조절, 랜덤 이미지를 사용과 같이 체스게임에서 체스 말이 가지고 있는 이미지를 변형하여 생기는 이미지를 게임내 그래픽으로 구성하여 체스 게임에서 게임봇 사용을 방지한다[23].

4.3 세부 알고리즘에 따른 분류

이상 징후 탐지의 경우 세부 알고리즘에 따라 분류가 가능하다. 기법에 따라 다양한 알고리즘이 사용되는데 본 절에서는 데이터 마이닝 기법에 대한 알고리즘과 튜링 테스트 기법에 대한 알고리즘을 나타내

었다. 기준이 되는 알고리즘은 Decision Tree, SVM, Naive Bayes, kNN, Logistic Regression, bayesian Network, Adaboost, Neural Network 로 나눌 수 있다. Table 5.는 세부 알고리즘에 따른 온라인 게임 관련 보안 연구들을 분류한 것이다.

Decision Tree는 특정 변수에 대해 여러 성질의 데이터를 유사한 성질의 데이터 끼리 분류하는 알고리즘이다. 또한 과거에 수집된 데이터들을 분석하여 유사한 그룹끼리 나누고 분류 모형을 나무 형태로 나타낸다. Hyungil Kim 등은 서버 단에서 사용자 행위를 데이터 마이닝 기법에 적용하여 게임봇 탐지 방법을 제시하였다. 제시한 방법론은 사용자가 게임을 플레이할 경우 키보드 및 마우스 입력 시 발생하는 윈도우 이벤트 메시지를 특징으로 추출하고, Decision Tree 알고리즘에 적용하여 MMORPG에서 게임봇을 탐지하였다[28].

SVM 알고리즘은 Decision Tree 알고리즘과 같이 여러 성질의 데이터를 유사한 성질의 데이터 끼리 분류하는 것으로 데이터가 사상된 공간에서 데이터 군을 나누는 경계는 경계면으로 나타난다. 이때 경계면의 최댓값을 찾는 것이 SVM 알고리즘이다. Ruck Thawonmas 등은 서버 단에서 캐릭터 행위 분석을 데이터 마이닝 기법에 적용하여 게임봇 탐지 방법을 제시하였다. 제시한 방법론은 캐릭터 행위에 대한 빈도를 특징으로 추출하고, SVM 알고리즘에 적용하여 MMORPG에서 게임봇을 분류하였다[25].

Naive Bayes 알고리즘은 특정 사건이 발생한 후 그 사건의 원인이 될 수 있는 사건들에 대한 사전 확률분포를 이용하여 사후에 원인이 될 수 있는 사건들의 사후확률분포를 도출하는 알고리즘이다. Ahmad Muhammad Aurangzeb 등은 서버 단에서 캐릭터들간의 네트워크 기반 데이터를 데이터 마이닝 기법에 적용하여 골드파머를 탐지하였다. 제시한 방법론은 캐릭터들간의 멘토링 네트워크, 거래 네트워크 및 게임 내의 가상 주택 소유자가 다른 캐릭터에게 접근 권한을 주어 형성되는 Housing-trust 네트워크를 피쳐로 추출하고, Naive Bayes, Bayesian Network, J48, KNN, Logistic Regression, Adaboost 알고리즘에 적용하여 MMORPG에서 골드파머를 분류하였다[20].

kNN 알고리즘은 학습 데이터 중 가장 유사한 k개의 데이터를 이용해 새로운 데이터의 부류 값을 예측하는 알고리즘이다. 이 알고리즘은 학습과정이 빠르고 효과적으로 분류하는 장점이 있지만 모든 데이터에 대해 거리 계산이 필요하기 때문에 데이터의 크기가 커짐에 따라 많은 소비 시간을 가지는 단점이 있다. Kuan-Ta Chen 등은 서버 단에서 캐릭터의 이동 패턴을 데이터 마이닝 기법에 적용하여 FPS에서 게임봇 탐지 방법을 제시하였다. 제시한 방법은 캐릭터의 이동 경로를 추적하여 특징으로 추출하고, kNN, SVM 알고리즘에 적용하여 게임봇을 분류하였다[26].

Logistic Regression 은 2개의 종속변수와 독립변수 사이의 관련성을 추정하는 통계 기법이다. 이 기법은 계산비용이 적고 결과 해석을 위한 표현이 쉬운 장점이 있지만 학습이 잘 되지 않은 모델의 경우 낮은 정확도를 가지는 단점이 있다. Hashem Alayed 등은 클라이언트 단에서 캐릭터의 행위를 데이터 마이닝 기법에 적용하여 FPS에서 Aim봇 탐지 방법을 제시하였다. 제시한 방법론은 게임 내 전투 시 타겟에 대한 조준 정확도, 적중률, 캐릭터의 이동패턴, 캐릭터와 타겟과의 거리 과 같은 특징을 추출하고, Logistic Regression 기법 및 SVM 알고리즘에 적용하여 Aim 봇을 탐지하였다[22].

Bayesian Network 그래프 이론과 확률 이론의 결합에 기초한 확률 그래프 모델이다. 이 알고리즘은 변수들 간의 상관관계를 쉽게 이해하는 것이 가능한 장점이 있지만 관련 없는 속성들에 대한 데이터 축소 과정이 필요한 단점이 있다. Jehwan Oh 등은 서버 단에서 캐릭터의 행위 및 소셜 네트워크 분석을 통해 MMORPG에서 게임봇을 탐지하였다. 제시한 방법론은 휴식시간, 휴식 횟수, 구매 횟수, 판매 횟수, 사냥으로 획득한 경험치 양, 길드 가입한 플레이어 수와 같은 캐릭터 행위에 대한 특징과 멘토링 네트워크와 같은 소셜 네트워크에 대한 특징을 추출하고, Bayesian Network, J48, kNN, Logistic Regression, Naive Bayesian, Adaboost 알고리즘에 적용하여 게임봇을 분류하였다[21].

Adaboost 알고리즘은 약한 분류기들을 선형으로 조합하고 반복을 통해 가중치 값을 추출하여 새로운 데이터의 부류 값을 예측하는 알고리즘이다. 이 알고리즘은 오류율이 낮고 빠른 연산 속도를 가지는 장점이 있지만 오류 데이터에 대해 민감한 단점이 있다. Muhammad Aurangzeb Ahmad 등은 서버 단에서 캐릭터의 행위 데이터를 데이터 마이닝 기법에

Table 5. Classification depending on a detection algorithm

Category	Research	Characteristic	Key research
Decision Tree	[8],[18],[20], [21],[28],[33], [44],[46]	- Easy to interpret of result - Low accuracy than relatively other classification algorithms	- “Detection of auto programs for MMORPGs“ [28]
SVM	[7],[13],[19], [22],[25-26], [36]	- Guarantee high accuracy of robustness for error data - Difficult to interpret of result	- “Detection of MMORPG bots based on behavior analysis” [25]
Naive Bayes	[8],[12],[20-21], [32-33]	- High accuracy depending on simple model and efficient calculation	- “Guilt by association? Network based propagation approaches for gold farmer detection” [20]
kNN	[8],[18],[20-21], [26],[33]	- Fast learning stage - Proportional relation between data size and computation time depending on calculation of distance in all of the data	- “Game bot identification based on manifold learning” [26]
Logistic Regression	[8],[20-22],[29], [33]	- Low computation - Easy to represent knowledge for interpreting of result - Low accuracy depending on underfitting	- “Behavioral-based cheating detection in online first person shooters using machine learning techniques” [22]
Bayesian Network	[8],[18],[21], [33],[34]	- Easy to understand correlation between features - Requiring data reduction of relationless attributes	- “Bot Detection Based on Social Interactions in MMORPGs” [21]
Adaboost	[8],[18],[21], [33]	- Low error rate and Fast computation speed - Sensitiveness in noise data	- “Mining for gold farmers: Automatic detection of deviant players in mmogs” [33]
Neural Network	[18],[27],[45]	- High accuracy and lots of computation time because of lots of computation quantities - Difficult to interpret grounds of result	- “The ones that got away: False negative estimation based approaches for gold farmer detection” [18]

적용하여 MMORPG에서 골드 파머 탐지 방법을 제시하였다. 제시한 방법론은 게임 내 캐릭터의 행위 시퀀스 패턴을 특징으로 추출하고, Adaboost, Bayes network, Naive Bayes, Logistic regression, J48, kNN 알고리즘에 적용하여 골드 파머를 탐지하였다[33].

Neural Network 알고리즘은 노드(Node)와 엣지(Edge)로 구성된 망구조를 모형화하고, 수집된 데이터를 반복 학습과정에 적용하여 패턴을 찾아 새로 입력되는 데이터의 부류 값을 예측하는 알고리즘이다. 이 알고리즘은 다른 알고리즘들에 비해 비교적 높은 정확도를 가지는 장점이 있지만 기준 근거를 알기 어렵고, 많은 연산량으로 인해 많은 소비시간과 분류 결과에 대한 기준 근거를 알기 어려운 단점이 있다. Atanu Roy 등은 서버 단에서 소셜 네트워크 데이터를 데이터 마이닝 기법에 적용하여 MMOG에서 골드파밍 그룹을 탐지하였다. 제시한 방법은 캐릭터 간의 거래, 그룹, 멘토 네트워크와 같은 소셜 네트워크 정보를 특징으로 추출하였고, 이를 MLP (Multilayer perceptron), Bayes Network, kNN, AdaBoost, J48 알고리즘에 적용하여 골드 파밍 그룹을 분류하였다[18].

4.4 데이터 소스에 따른 분류

이상 징후 탐지는 데이터 소스에 따라 분류가 가능하다. 기준이 되는 데이터 소스는 캐릭터 행위, 캐릭터 이동 경로, 사용자 행위, 소셜 네트워크 데이터, 네트워크 트래픽 데이터, 이미지 소스로 나눌 수 있다. Table 6.는 데이터 소스에 따른 온라인 게임

Table 6. Classification depending on a data source

Category	Research	Characteristic	Key research
Character behavior	[9],[12-17], [19],[22], [24-25],[32-34], [36],[38], [40-41]	- Easy to classification between normal character and abnormal character because of different behavior - Requiring lots of data source because of high accuracy	- “Online game bot detection based on party-play log analysis” [15]
Character travel path	[6],[11],[26], [37],[48]	- Easy to classification because of difference of travel path each to each - Requiring differential application depending on using map	- “Second life: a social network of humans and bots” [10]
User behavior	[13],[28],[36-37],[41-42],[46]	- Easy to classification because of difference of Window event between normal user and abnormal user - Requiring client module to analysis	- “An automatic and proactive identity theft detection model in MMORPGs” [36]
Social network	[7],[8],[10], [18],[20-21], [27],[29], [30-31],[39]	- Applicable in online game, easy to classification between normal user and abnormal user - Difficult to classification between normal user and abnormal user in solo play game	- “Battle of botcraft: fighting bots in online games with human observational proofs” [27]
Network traffic	[43-45]	- Enable using without modifying in server and client - Enable fast response for abnormal user in case of leak of detection rule	- “A modern turing test: Bot detection in MMORPGs” [45]
Image source	[23],[35],[47]	- Small computation and resource because of image source - Falling of game immersion in game playing	- “Preventing bots from playing online games” [47]

관련 보안 연구들을 분류한 것이다.

캐릭터 행위는 게임 플레이 시 서버에 저장되는 캐릭터 행위 로그이다. 캐릭터 행위 로그는 액션행위 시퀀스, 경험치 획득, 로그인 및 로그아웃 데이터, 획득 재화, 상점 이용 횟수, 승리 비율, 조준정확도, 타겟과의 거리와 같은 데이터이다. Ah Reum Kang 등은 서버 단에서 일반 캐릭터들이 파티 플레이를 통해 얻게 되는 경험치, 획득한 아이템, 획득한 재화, 파티 플레이 시간, 시간에 따른 파티원의 변화를 특징으로 추출하고 통계적 기법에 적용하여 MMORPG에서의 게임봇을 탐지하였다[15]. Mee Lan Han 등은 서버 단에서 캐릭터의 승리 비율, 헤드샷 비율, 플레이 시간, 게임 재화 및 경험치 변화량, 연속 승리 비율을 특징으로 추출하고, 통계적 기법에 적용하여 FPS에서 게임봇을 탐지하였다[16].

캐릭터 이동경로는 게임 플레이 시 캐릭터가 이동한 경로를 추적한 데이터이다. 일반 캐릭터와 다르게 이상 행위를 하는 캐릭터의 경우 특정 지역만 이동하거나 반복적으로 동일 구간만 이동하는 등 일반 캐릭터와는 다르게 이동하므로 이를 이상 징후 탐지에 데이터 소스로 사용된다. Matteo Varvello 등은 서버 단에서 일반 사용자간의 연결성이 일반 사용자와 게임봇간의 연결성보다 강하게 구성되어있는 차이점을 특징으로 추출하고, 통계적 기법에 적용하여 게임봇을 분류하였다[10].

사용자 행위는 게임 플레이 시 사용자가 입력하는 키보드 입력, 마우스 클릭, 마우스 움직임, 사용자 접속 IP 주소, 해당 PC MAC 주소와 같은 데이터이다. Jiyoung Woo 등은 서버 단에서 캐릭터 및

사용자 행위 데이터를 데이터 마이닝 기법에 적용하여 MMORPG에서 계정도용 탐지 방법을 제시하였다. 제시한 방법론은 연결한 유저의 IP 주소, MAC 주소 와 같은 연결 정보와 로그인 시간, 거래 금지를 당한 시간, 보유 재화의 감소, 보유 경험치의 증가와 같은 캐릭터의 행위 분석을 특징으로 추출하고, SVM 알고리즘에 적용하여 MMORPG에서 계정도용을 탐지하였다[36].

소셜 네트워크 데이터는 게임 플레이 시 서버에 저장되는 캐릭터의 소셜 행위 및 네트워크 데이터이다. 사용되는 데이터는 캐릭터의 채팅, 거래, 파티, 길드, 멘토링, PVP와 같은 소셜 네트워크 관련 데이터이다. Steven Gianvecchio 등은 서버 단에서 사용자 행위 데이터를 데이터 마이닝 기법에 적용하여 게임봇 탐지 방법을 제시하였다. 제시한 방법론은 마우스 클릭, 키보드 입력, Drag&Drop과 같은 사용자가 게임 플레이할 경우에 발생하는 행위를 특징으로 추출하고, Neural Network 알고리즘에 적용하여 MMOG에서 게임봇을 탐지하였다[27].

네트워크 트래픽은 게임 플레이 시 서버와 클라이언트간의 전송되는 패킷 사이즈, 종류, 빈도, 타이밍과 같은 데이터를 의미한다. Adam Cornelissen 등은 네트워크 단에서 네트워크 트래픽을 데이터 마이닝 기법에 적용하여 MMORPG에서 게임봇 탐지 방법을 제시하였다. 제시한 방법론은 새로운 세션 연결, 캐릭터의 위치 이동, 캐릭터의 방향 변화, 아이템 습득, 공격에 대한 게임 내 캐릭터들의 행위에 따라 발생하는 네트워크 패킷의 수를 특징으로 추출하고, Neural Network 알고리즘에 적용하여 게임봇을 탐지하였다[45].

이미지 소스는 카드 게임에서 게임 내 카드의 그림을 방향 회전하거나 이미지 변형을 하거나, 게임에서 CAPTCHA를 위한 사진에 문자열로 표시되어 사용된다. Golle Philippe 등은 클라이언트 단에서 튜링테스트를 통해서 게임봇 예방 방법을 제시하였다. 제시한 방법은 게임을 이용하는 유저가 사람인지 게임봇인지를 판단하기 위해 사용하는 CAPTCHA 이미지를 카드 게임에 적용한 것이다[47].

4.5 게임 장르에 따른 분류

이상 징후 탐지는 온라인 게임 장르에 따라 분류가 가능하다. 기준이 되는 온라인 게임 장르는 MMORPG, FPS, 카드 게임, 경주 게임(racing game)으로 나눌 수 있다. Table 7.은 게임 장르에 따른 온라인 게임 관련 보안 연구들을 분류한 것이다.

MMORPG (Massive Multiplayer Online Role Playing Game)는 대규모 다중사용자 온라인 롤 플레잉 게임의 줄임말로 게임 속의 캐릭터들을 설정하여 온라인상에서 여러 사용자들이 같은 가상공간에서 동시에 즐길 수 있는 게임이다. Chung Yeounoh 등은 서버 단에서 게임 캐릭터의 행위를 데이터 마이닝 기법에 적용하여 게임봇 분류 방법을 제시하였다. 제시한 방법론은 사냥, 공격, 방어, 회피, 회복과 같은 캐릭터의 전투 관련 패턴과 수집패턴, 이동 패턴을 피쳐로 추출하고, SVM 알고리즘에

Table 7. Classification depending on a game genre

Category	Research	Characteristic	Key research
MMORPG	[6-12],[14-15], [17-21],[25], [27-33],[36], [39-46],[48]	- High degree of freedom in the game - Appearing a variety of user-specific features - Enable playing of cooperation - High initial entry barrier of game	- “Game Bot Detection Approach Based on Behavior Analysis and Consideration of Various Play Styles” [19]
FPS	[12],[15],[22], [24-25],[34], [37]	- Game playing of combat between peoples - Requiring fast response speed in game playing - High initial entry barrier of game	- “A statistical aimbot detection method for online FPS games” [24]
Card Game	[23],[35],[47]	- Low initial entry barrier of game	- “Embedded noninteractive continuous bot detection” [35]
Racing Game	[38]	- Requiring to understand for game play map - Low initial entry barrier of game	- “Win, lose or cheat: The analytics of player behaviors in online games” [38]

적용하여 MMORPG에서 게임봇을 분류하였다[19]. Ah Reum Kang 등은 서버 단에서 캐릭터의 채팅 행위를 데이터 마이닝 기법에 적용하여 게임봇 탐지 방법을 제시하였다. 제시한 방법론은 채팅 크기, 빈도, 채팅 종류, 채팅하는 사람, 채팅 위치와 같은 채팅 관련 특징을 추출하고, Random forest, Logistic regression, Lazy learning 알고리즘에 적용하여 MMORPG에서 게임봇을 탐지하였다[29]. Hyukmin Kwon 등은 서버 단에서 캐릭터들간의 단방향 거래 네트워크 분석을 통계적 기법에 적용하여 MMORPG에서 게임봇을 탐지하였다[30].

FPS (First-person shooter)는 게임 내 캐릭터의 시점을 1인칭 시점에서 바라보며 게임의 목적을 수행하는 게임이다. Su-Yang Yu 등은 서버 단에서 캐릭터 행위 분석을 이용하여 FPS에서 Aim봇을 탐지하는 방법을 제시하였다. 제시한 방법론은 타겟을 조준하는데 걸리는 마우스 커서의 속도, 타겟을 조준하는데 걸리는 시간 등과 같은 캐릭터 행위에 대한 특징을 추출하고, 통계적 기법에 적용하여FPS에서 Aim봇을 분류하였다[24]. S.F. Yeung 등은 서버 단에서 캐릭터의 행위 데이터를 데이터 마이닝 기법에 적용하여 Aim봇 탐지 방법을 제시하였다. 제시한 방법론은 캐릭터의 움직임 타겟 조준의 정확성, 조준 거리를 특징으로 추출하고, Bayesian Network 알고리즘에 적용하여 FPS에서 Aim봇을 탐지하였다[34].

카드 게임은 게임 내에서 주어지는 카드를 이용하여 게임 상에서 다른 캐릭터들과의 경쟁에서 이기는 보드게임의 한 종류이다. Roman V. Yampolskiy 등은 온라인 카드 게임에서 튜링테스트 기법의 CAPTCHA를 적용하여 게임 내 게임봇을 예방하는 방법을 제안하였다[35].

경주 게임은 게임속 캐릭터와 다른 캐릭터들간 스피드 경쟁을 통해 출발점에서 시작하여 결승점까지 이동하는 게임이다. Johanne Christensen 등은 서버 단에서 캐릭터의 행위 분석을 통계적 기법에 적용하여 게임핵 탐지 방법을 제시하였다. 제시한 방법론은 레이싱 게임에서 경주 대상의 경주 속도 및 시간을 클라이언트와 서버에서의 비교하고, 통계적 기법에 적용하여 경주 게임에서 게임핵을 탐지하였다[38].

4.6 탐지 대상에 따른 분류

이상 징후 탐지는 탐지 대상에 따라 분류가 가능하다. 기준이 되는 탐지 대상은 게임봇 탐지, 게임봇 예방, 게임핵 탐지, 계정도용 탐지, 골드파밍 그룹 탐지로 나눌 수 있다. Table 7.은 탐지 대상에 따른 온라인 게임 관련 보안 연구들을 분류한 것이다.

Table 8. Classification depending on a detection target

Category	Research	Characteristic	Key research
Game bot detection	[6],[9-13], [15-17],[19], [21-22],[24-32], [34],[40],[43], [44-46],[48]	- Pattern detection of repetitive behavior for specific purpose	- “I know what the BOTs did yesterday: Full action sequence analysis using Naïve Bayesian algorithm” [32]
Gold farming group detection	[7-8],[18],[20], [33],[39],[42]	- Using feature of character transaction data - Detection through using the most of social network data	- “What can free money tell us on the virtual black market?” [39]
Account steal detection	[14],[36-37], [41]	- Detection through using the most of user access information and login data	- “Trajectory based behavior analysis for user verification” [37]
Game bot prevention	[23],[35],[47]	- Using the most of Turing Test technique - Access control for another program through game security solution	- “Preventing bots from playing online games” [47]
Game hack detection	[38]	- Using game security solution	- “Win, lose or cheat: The analytics of player behaviors in online games” [38]

게임봇 탐지는 서버에 저장 가능한 캐릭터 행위, 이동 경로, 사용자 행위, 소셜 네트워크 데이터, 네트워크 트래픽 데이터를 분석하여 게임 속에서 사용자 대신 게임을 플레이 해주는 자동화된 프로그램을 탐지하는 것이다. Sang-Hyun Park 등은 서버 단에서 타겟 사냥 지속시간, 마을에서 머무르는 시간, 사냥시의 휴식 상태, 맵의 변화, 획득 경험치와 같은 캐릭터의 행위 분석을 특징으로 추출하고, 통계적 기법에 적용하여 MMORPG에서 게임봇을 탐지하였다[31]. Jina Lee 등은 서버 단에서 캐릭터 행위 분석을 데이터 마이닝 기법에 적용하여 게임봇 탐지 방법을 제시하였다. 제시한 방법론은 게임 내에서 캐릭터의 행위 시퀀스를 특징으로 추출하고, Naive Bayesian 기법에 적용하여 MMORPG에서 게임봇을 탐지하였다[32]. Hyukmin Kwon 등은 서버 단에서 캐릭터 행위 분석을 유사도 패턴 매칭 기법에 적용하여 게임봇 탐지 방법을 제시하였다. 제시한 방법은 캐릭터의 행위 시퀀스를 특징으로 추출하고, Cosine similarity 알고리즘에 적용하여 MMORPG에서 게임봇을 탐지하였다[40].

골드파밍 그룹 탐지는 게임 내 대규모의 게임봇을 이용하여 게임 재화를 획득하는 작업장을 탐지하는 방법으로 서버에 저장되는 로그를 통해 이루어진다. Kyungmoon Woo 등은 서버 단에서 거래 네트워크 중 대가 없는 게임 재화 거래에 대한 특징을 통계적 기법에 적용하여 MMORPG에서 골드파밍 그룹을 탐지하였다[39]. Dongnam Seo 등은 서버 단에서 유저 행위 정보를 데이터 마이닝 기법에 적용하여 골드파밍그룹 탐지 방법을 제시하였다. 제시한 방법론은 유저의 접속 IP 주소, 계정명, 국가코드 등과 같은 정보를 특징으로 추출하고, k-means 알고리즘에 적용하여 골드파밍그룹을 탐지하였다[42].

계정도용 탐지는 게임 사용자의 계정을 탈취하여 불법 로그인 수행과 같은 부정행위를 탐지하는 방법으로 서버에 저장되는 게임 플레이 로그를 이용하여 탐지한다. Pao Hsing-Kuo 등은 서버 단에서 유저 행위 분석을 데이터 마이닝 기법에 적용하여 계정도용 탐지 방법을 제시하였다. 제시한 방법론은 게임 내 캐릭터의 이동경로 및 사용자의 마우스 경로 추적을 특징으로 추출하고, HMM 알고리즘에 적용하여 FPS에서 계정도용을 탐지하였다[37]. Hwa Jae Choi 등은 서버 단에서 캐릭터의 접속 IP 주소 와 같은 유저 행위 정보 및 아이템 판매 횟수, 경험치 획득, 캐릭터 레벨, 게임 플레이 시간, 캐릭터내 재화 감소 비율, 개인 상점 이용 횟수등 캐릭터 행위 정보를 특징으로 추출하고, 통계적 기법에 적용하여 MMORPG에서 계정도용을 탐지하였다[41].

게임봇 예방은 사전에 게임봇의 사용을 막는 것으로 게임 클라이언트 실행 시 게임 보안 솔루션을 적용하여 다른 프로그램의 접근을 제어한다. 다른 방법으로 게임 기획 시 게임 내부의 튜링테스트 기법을 적용하여 게임봇의 이용을 방해하는 방법이다[22][35][47].

게임핵 탐지는 서버에 저장되는 로그를 이용하여 게임 내 스피드 핵, 월 핵, 맵 핵 등과 같이 메모리 조작 또는 네트워크 패킷 조작을 통해 이루어지는 부정행위를 막는 방법이다[38].

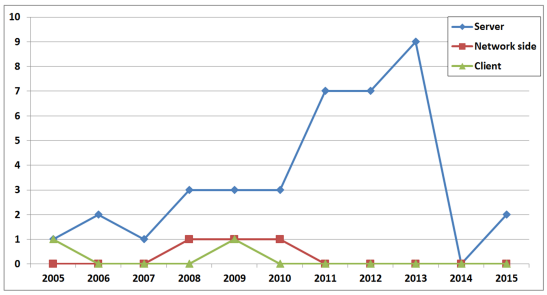
V. 고 찰

Fig 2.는 분류 기준에 따른 연도별 온라인연구 분포를 나타낸 것이다. (a)는 탐지 단에 따른 연도별 연구 분포를 나타낸 것으로 2005년부터 2013년까지 서버 단에서의 탐지하는 연구가 많이 진행되었고, 네트워크 단과 클라이언트 단에서는 많이 진행되지 않은 것을 알 수 있다. 서버, 네트워크, 클라이언트 단에서의 연구 중 서버 단에서의 연구가 많이 이루어진 것은 데이터 수집 및 분석이 용이하고, 분석 자원 및 속도의 저하를 일으키지 않은 장점이 있기 때문인 것으로 볼 수 있다.

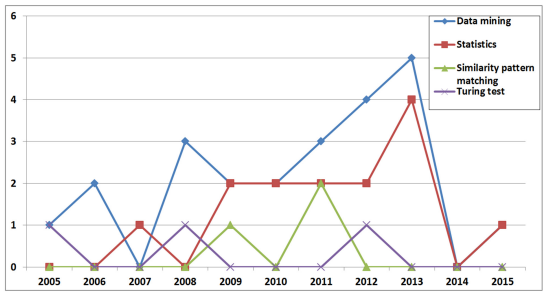
(b)는 탐지 기법에 따른 연도별 연구 분포를 나타낸 것으로 데이터 마이닝 기법과 통계적 기법이 꾸준히 증가한 것을 확인할 수 있다. 데이터 마이닝 기법, 통계적 기법, 유사도 패턴 매칭 기법, 튜링 테스트 기법 중 데이터 마이닝 기법을 적용한 연구가 많이 이루어진 것은 시간이 흐르면서 게임 플레이 로그의 양이 많아짐에 따라 분석하기 용이하고 상대적으로 다른 기법들에 비해 높은 정확도를 가지는 장점이 있기 때문인 것으로 볼 수 있다.

(c)는 탐지 알고리즘에 따른 연도별 연구 분포를 나타낸 것으로 Decision Tree와 SVM 알고리즘이 많은 연구에서 사용 되었다. 그 이유로 Decision Tree는 결과에 대한 해석이 가능하고 연산속도가 빠르다는 장점이 있고 SVM은 결과에 대한 해석이 어렵지만 다른 알고리즘들에 비해 정확도가 높은 장점이 있기 때문인 것으로 볼 수 있다.

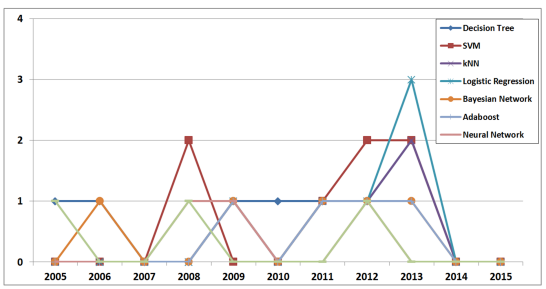
(d)는 데이터 소스에 따른 연도별 연구 분포를 나타낸 것으로 캐릭터 행위 데이터가 많이 사용 되었으



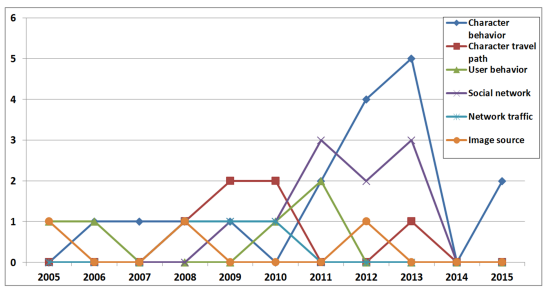
(a) Distribution of annual research depending on a detection side



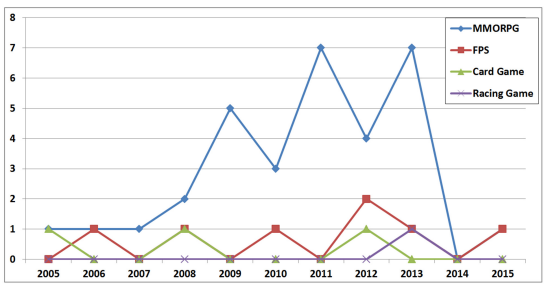
(b) Distribution of annual research depending on a detection technique



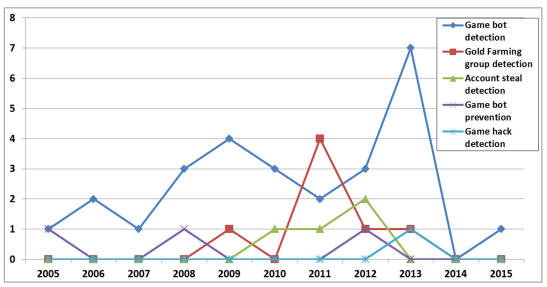
(c) Distribution of annual research depending on a detection algorithm



(d) Distribution of annual research depending on a data source



(e) Distribution of annual research depending on a game genre



(f) Distribution of annual research depending on a detection target

Fig. 2. Distribution of annual research depending on criteria for classification

며 그 외 소셜 네트워크 데이터 및 사용자 행위 데이터가 많은 연구에서 사용된 것을 알 수 있다. 데이터 소스 중 캐릭터 행위 데이터를 이용한 연구가 많이 이루어진 것은 사용자들의 습관적 행동을 게임 속 캐릭터가 많은 부분에서 나타내기 때문인 것으로 생각할 수 있다. 두 번째로 많이 이용된 데이터 소스는 소셜 네트워크 데이터로 게임봇 및 골드파밍 그룹과 같이 게임 재화를 획득하여 현금교환을 위해 거래 행위 및 소셜 네트워크를 형성할 경우 쉽게 비교가 가능하기 때문인 것으로 생각할 수 있다.

(e)는 게임 장르에 따른 연도별 연구 분포를 나타낸 것으로 많은 연구가 MMORPG 게임 장르에서 이루어졌고, 그 외에 FPS에서 이루어진 것을 알 수 있다. 게임 장르 중 MMORPG 장르에 대해 연구가 많이 이루어진 것은 MMORPG의 게임 내 자유도가 높아 사용자별 다양한 특징이 나타나고, 유명 MMORPG 게임의 경우 게임봇을 이용한 부정행위가 많이 일어나기 때문에 이를 탐지하기 위한 것으로 볼 수 있다.

(f)는 탐지 대상에 따른 연도별 연구 분포를 나타낸 것으로 게임봇 탐지 부분에서 많은 연구가 이루어졌고, 그 다음으로 골드파밍 그룹 탐지, 계정도용 탐지 순으로 연구가 된 것을 확인할 수 있다. 다양한 탐지 대상 중 게임봇 탐지에 대해 많은 연구가 이루

어진 것은 게임봇의 경우 특정 목적을 가지기 때문에 반복적인 행위에 대한 분석을 통해 보다 쉽게 분류할 수 있고, 게임봇을 이용한 게임속 재화 획득 및 현금 교환이 가능하고 온라인 게임 회사의 게임봇 사용으로 인한 손실을 방지하기 위한 것으로 생각할 수 있다.

Fig 1.을 통해 온라인 게임 시장의 규모와 모바일 게임 시장의 규모를 생각해보면 모바일 게임 시장에서 부정행위가 크게 성장할 것으로 보인다. 하지만 이에 따른 모바일 게임에 대한 연구는 많이 이루어지지 않았는데 그 이유를 세 가지 정도로 생각해 볼 수 있다. 첫째, 모바일 게임은 게임의 생명 주기가 짧아 부정행위가 발생할 만한 환경이 구성되지 않는다. 모바일 게임의 생명 주기는 짧으면 2~3달 정도로 그 이상의 기간이 지나게 되면 사용자들이 다른 게임으로 옮겨가기 때문에 부정행위자들은 목표 대상을 잃어버리게 된다. 둘째, 게임 내 사용자들의 아이템 거래가 이루어지지 않는다. 이는 게임 캐릭터 간의 교환이 이루어지지 않기 때문에 게임봇을 이용한 아이템을 획득하더라도 이를 이용한 현금 교환이 불가능하다. 셋째, 모바일 게임 내 NPC에게 아이템을 구매할 경우 게임 내 재화 또는 실제 현금으로 결제를 해야 얻을 수 있다. 이와 같은 이유로 인해 모바일 게임에서 부정행위에 대한 탐지 및 예방 연구가 많이 진행되지 않은 것으로 보인다.

모바일 게임은 향후 게임 내 사용자들간 아이템 거래 활성화가 이루어질 경우 이를 통한 게임 내 게임봇 사용수가 많아질 것이기 때문에 모바일 환경에서의 게임봇 탐지 관련 연구가 진행되어야 할 것으로 보인다. 또한 현재 모바일 게임의 특성상 온라인게임과는 다르게 결제부정이 많이 이루어지고 있기 때문에 이를 예방 및 탐지 가능한 연구가 이루어져야 할 것으로 보인다.

VI. 결 론

온라인 게임 시장 성장과 더불어 이를 이용한 부정행위 역시 빠르게 성장해 왔다. 부정행위는 게임회사와 게임 이용자 모두에게 많은 피해를 입히고 있다. 이를 방지하기 위해서 게임 보안 솔루션과 같은 제품을 설치하여 대응하고 있다. 하지만 게임 보안 솔루션으로 부정행위를 완벽하게 막는 것에는 어려움이 있다. 게임별 이루어지는 부정행위가 다르고 이를 막기 위해서는 다양한 방법과 시각에서 보안이 행해져야 한다. 또한 게임 기획과 함께 조화 가능한 보안 솔루션의 적용 되어야 한다.

본 논문에서는 온라인 게임에서의 부정행위 및 부정행위 탐지 및 예방 관련 연구들을 조사하였다. 조사한 연구들을 탐지 단, 탐지 기법, 탐지 알고리즘, 적용한 데이터 소스, 게임 장르, 탐지 대상과 같이 6개의 분류기준을 통해 분류하였다. 또한 분류 기준에 따른 연도별 연구 분포와 플랫폼별 시장 규모를 통해 향후 연구가 필요한 분야에 대해 논의 하였다.

향후 플랫폼 변화에 따라 부정행위의 형태가 변화하면 과거의 탐지 및 예방 관련 연구들의 적용이 어려울 수 있기 때문에 다양한 환경에서의 대응 연구가 이루어 져야 할 것이다.

References

[1] Newzoo, “2014 Global games Market Report”

[2] AhnLab, “ASEC Report,” vol.59, Nov. 2014

[3] Jeff Yan, Jianxin, and Hyun-Jin Choi, “Security issues in online games,” The Electronic Library, vol. 20, no. 2, pp. 125-133, 2002

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

[5] 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

[6] 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

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

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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

[14] 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

[15] 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

[16] 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

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

[18] 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

[19] 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

[20] 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

[21] 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

[22] 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
〔23〕 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
〔24〕 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
〔25〕 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
〔26〕 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
〔27〕 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
〔28〕 Hyungil Kim, Sungwoo Hong and Juntae Kim, "Detection of auto programs for MMORPGs," Advances in Artificial Intelligence, pp. 1281-1284, Dec. 2005
〔29〕 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
〔30〕 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
〔31〕 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
〔32〕 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
〔33〕 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
〔34〕 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
〔35〕 Roman V. Yampolskiy and Venu Govindaraju, "Embedded noninteractive continuous bot detection," Computers in Entertainment, vol. 5, no. 4, 2008
〔36〕 Jiyoung Woo, Hwa Jae Choi and Huy Kang Kim, "An automatic and proactive identity theft detection model in MMORPGs," Appl. Math, vol. 6, no. 1, pp. 291-302, 2012
〔37〕 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
〔38〕 Christensen Johanne, Oleg Veryovka and

Ben Watson, "Win, lose or cheat: The analytics of player behaviors in online games," TR-2013-5, Computer Science, North Carolina State University, 2013

[39] 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

[40] 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

[41] 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

[42] 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

[43] Kuan-Ta Chen, Jiang Jhih Wei, Huang Polly, Chu Hao Hua, Lei Chin Laung and Chen Wen Chin, "Identifying MMORPG bots: A traffic analysis approach," EURASIP Journal on Advances in Signal Processing, vol. 2009, no. 3, Jan. 2009

[44] 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

[45] Adam Cornelissen and Franc Grootjen, "A modern turing test: Bot detection in MMORPGs," Belgian-Dutch Conference on Artificial Intelligence, pp. 49-55, Oct. 2008

[46] Sungwoo Hong, Hyungil Kim and Juntae Kim, "Identification of Auto Programs by Using Decision Tree Learning for MMORPG," Journal of Korea Multimedia Society, 9(7), pp. 927-937, July 2006

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

[48] 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

〈저자소개〉

곽 병 일 (Byung Il Kwak) 정회원
2013년 2월: 세종대학교 컴퓨터공학과 졸업
2013년 9월~현재: 고려대학교 정보보호학과 석·박사통합과정
〈관심분야〉 온라인게임 보안, 데이터 마이닝, 네트워크 보안, IoT 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~2014년 12월: 고려대학교 정보보호대학원 조교수
2015년 1월~현재: 고려대학교 정보보호대학원 부교수
〈관심분야〉 온라인게임 보안, 네트워크 보안, 네트워크 포렌식