Journal of Korea Game Society 2015 Jun; 15(3): 177-188
http://dx.doi.org/10.7583/JKGS.2015.15.3.177

온라인 게임 보안

사용자 로그 분석을 통한 FPS 게임에서의 치팅 사용자 탐지 연구: 인공 신경망 알고리즘을 중심으로

박정규, 한미란, 김휘강
고려대학교 정보보호대학원
{pjk0825, blosst, cenda}@korea.ac.kr

A Study of Cheater Detection in FPS Game by using User Log Analysis

Jung Kyu Park, Mee Lan Han, Huy Kang Kim
Graduate School of Information Security, Korea University

요 약

온라인 게임의 인기 장르인 FPS (First Person Shooting) 게임에서 치팅(cheating)을 근절하기 위해 게임 회사는 다양한 클라이언트 보안 솔루션을 운영하고 있지만 불법 프로그램을 이용한 치팅은 끊이지 않고 있으며 이로 인한 피해도 지속적으로 발생하고 있다. 본 논문에서는 서버 단에서 게임 로그 분석을 통해 FPS 게임의 치팅 사용자를 탐지하는 방법을 제안한다. FPS 게임에서 일반적으로 적재되는 로그를 중심으로 치팅 사용자와 일반 사용자의 특성을 비교 분석하고 인공 신경망 알고리즘을 이용해 치팅 사용자를 탐지하는 모델을 생성하였다. 또한 실제 서비스 중인 FPS 게임 로그를 이용해 치팅 사용자 탐지 모델에 대한 성능 평가를 수행하였다.

ABSTRACT

In-game cheating by the use of unauthorized software programs has always been a big problem that they can damage in First Person Shooting games, although companies operate a variety of client security solutions in order to prevent games from the cheating attempts. This paper proposes a method for detecting cheaters in FPS games by using game log analysis in a server-side. To accomplish this, we did a comparative analysis of characteristics between cheaters and general users focused on commonly loaded logs in the game. We proposed a cheating detection model by using artificial neural network algorithm. In addition, we did the performance evaluation of the proposed model by using the real dataset used in business.

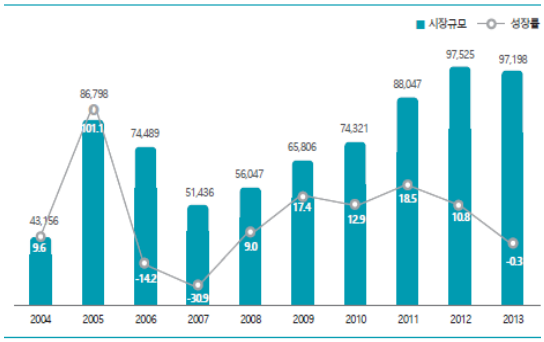
Keywords : Online Game Security, Cheating Detection, Data mining, Log Analysis

Received: Apr. 20, 2015 Accepted: Apr. 29, 2015
Corresponding Author: Huy Kang Kim (Korea University)
E-mail: cenda@korea.ac.kr

ISSN: 1598-4540 / eISSN: 2287-8211

1. 서 론

온라인 게임 시장은 인터넷 보급의 가장 큰 수혜자라고 할 수 있을 만큼 1990년대 이후 급격하게 성장하였고 주요 문화 산업으로 자리매김하였다. 최근 정부의 게임 규제 시도가 계속되면서 온라인 게임 시장 규모가 다소 하락했지만 2013년 국내 온라인 게임 시장 규모는 5조 4천억원을 기록했으며 이는 전체 게임시장의 56.1%를 차지한다. [Fig. 1]은 국내 게임 시장의 동향을 보여준다[1].



[Fig. 1] Trends of Korean Game Market (2004~2013)

FPS는 온라인 게임 분야에서 가장 인기 있는 게임 장르 중 하나이다. 1인칭 슈팅 게임으로 총을 이용해 상대편을 모두 제압하면 승리하게 된다. 상대의 위치를 파악하고 상대와 마주했을 때 먼저 조준하고 공격하는 것이 게임을 이기기 위한 핵심 포인트이다. 일부 사용자들은 게임에서 승리하기 위해 불법 프로그램을 사용해 치팅 행위를 한다. 불법 프로그램은 종류에 따라 다양한 치팅 기능을 제공하며 일반적으로 많이 알려진 치팅 프로그램으로는 상대편과 마주했을 때 상대 캐릭터를 자동으로 조준해주는 AimBot, 벽이나 장애물 등을 관통하여 다른 사용자를 볼 수 있게 해주는 WallHack, 무기의 기본 속성을 변경하거나 사용자가 구매하지 않은 무기를 자유자재로 사용할 수 있게 해주는 WeaponHack 등이 있다[2].

이러한 치팅 행위를 하는 사용자는 상대와의 교전에서 우위를 점할 수 있고, 게임시 조작의 편리함을 느낄 수 있지만, 일반 사용자와 게임 회사는 심각한 피해를 받게 된다. FPS 게임의 특성상 치팅 사용자가 상대 사용자에게 직접적인 영향을 미쳐 게임 이탈과 같은 2차적인 피해로 이어지기 쉬우며, 게임의 신뢰도를 하락시키고 게임 라이프 사이클을 단축시키는 등의 피해를 발생시키게 된다[3,4].

게임 회사는 치팅을 차단하기 위한 노력으로 GameGuard, Hackshield와 같은 클라이언트 기반의 보안 솔루션을 운영하고 있다. 하지만 이러한 클라이언트 기반의 탐지 방법은 프로세스 인젝션, 프로세스 우회와 같은 기법으로부터 100% 안전할 수 없으며, 다른 프로그램과의 충돌을 발생시켜 사용자 편의성을 떨어뜨릴 수 있다. 또한 새로운 치팅 프로그램을 탐지하기 위해서는 지속적인 패치가 필요하다[5].

사용자 행위 분석을 통한 치팅 탐지 방법도 연구되고 있지만 FPS의 경우 치팅 프로그램이 완전히 독립적으로 동작하지 않고 사용자의 플레이에 보조적인 역할을 수행하므로 일반 사용자와 치팅 사용자를 구별하기 위한 특징 추출이 어렵다[6]. 또한 FPS는 게임 속도가 중시되므로 게임랙을 발생시킬 수 있는 추가적인 작업은 적용하기 어렵고, 발생하는 이벤트 횟수가 많아 모든 사용자의 행위 로그를 서버에 적재하는 것이 현실적으로 불가능하다. 기존 사용자 행위 기반의 연구들은 서버에 적재되지 않는 로그를 사용한 경우가 많으며, 이 경우 실제 서비스에 적용이 어렵다는 한계가 있다.

본 논문에서는 기존 탐지 방법들의 문제점을 해결하기 위한 방법으로, 서버 단에서 게임 로그 분석을 통해 치팅 사용자를 탐지하는 프레임워크를 제안하였다. 실제 서버에 적재되는 로그를 중심으로 일반 사용자와 치팅 사용자의 차이점을 비교분석하였고 치팅 사용자 그룹을 분류하기 적합한 피쳐(feature)들을 선정하였다. 그리고 인공 신경망 알고리즘을 이용해 탐지 모델을 생성하고 탐지 성능을 평가하였다.

2. 관련 연구

온라인 게임에서 치팅으로 인한 피해는 오래전부터 지속적으로 발생해왔고 이로 인해 온라인 게임에서 보안은 주된 관심의 대상이 되었다. 기존의 연구는 MMORPG(Massive Multiplayer Online Role Playing Game)를 대상으로 한 연구가 주를 이루었으며 다양한 부정행위 탐지 방법에 대한 연구가 진행되어 왔다. Kang 등[3]은 MMORPG에서의 게임봇 탐지 방법을 사용자 행위 기반[7][8][9], 이동 경로 기반[10], 트래픽 기반[11], HOP 기반[12], CAPTCHA 기반[13]의 5 가지 방법으로 분류하였다. 하지만 FPS 게임은 MMORPG와는 다른 장르의 게임으로 게임의 플레이 방식이 달라 기존의 탐지 방법에 대한 적용이 불가능한 경우가 존재한다. 예를 들어 FPS 게임은 1인칭 슈팅 게임으로 게임 플레이 중 사용자에게 튜링 테스트를 진행하는 CAPTCHA와 같은 방식은 적용이 불가능하다.

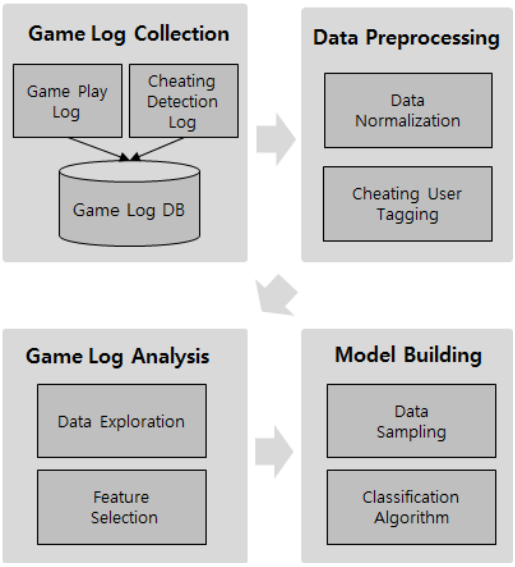
FPS 게임에서 기존의 치팅 탐지 연구는 크게 이동 경로 기반과 사용자 행위 기반의 두 가지 방법으로 연구되어 왔다. 이동 경로 기반의 탐지 방법은 일반 사용자와 치팅 사용자의 이동경로 차이가 존재할 것이라고 가정하는 방법으로 Chen 등[14]은 사용자의 이동경로를 Isomap을 이용해 데이터의 차원을 축소하고 SVM과 KNN 알고리즘을 이용하는 탐지 방법을 제안하였다. Quake2 게임을 수정하여 실험을 진행하였고 700초의 추적을 통해 98%의 높은 탐지 성능을 보였다. 하지만 Kesteren 등[10]은 Chen 등[14]의 논문에서 이동경로 비교에 사용한 피쳐가 봇 개발자에 의해서 쉽게 수정될 수 있다고 지적하였다.

사용자 행위 기반의 탐지 방법은 일반 사용자와 치팅 사용자의 행동 차이를 이용하는 방법이다. Galli 등[15]은 치팅 사용자 탐지를 위한 프레임워크를 제안하였으며 5 가지 Machine Learning 알고리즘(SVM, Neural Networks, Decision Tree, Random Forest, Naive Bayes)을 적용하여 치팅 사용자 탐지 실험을 수행하였다. Alayed 등[4]은 치팅 사용자 탐지를 위한 최적의 피쳐를 찾기 위해 다양한 피쳐들의 조합으로 실험을 진행하였고 탐지 성능이 우수한 피쳐들의 순위를 제공하였다. Yu 등[6]은 AimBot 사용자를 탐지하기 위한 두 가지 피쳐를 소개하였고 투표 시스템을 제안하였다. Alayed 등[4]와 Yu 등[6]의 연구를 통해 타겟을 조준하는 시간과 조준을 유지하는 지속시간이 AimBot 사용자를 탐지하는 효과적인 피쳐로 확인되었다. 하지만 해당 피쳐는 게임 속도가 중요한 FPS 게임의 특성상 로그가 서버에 저장되지 않고 있으며 제안하는 탐지 방법을 대규모의 FPS 게임 서비스에 적용하기 어렵다는 한계가 있다.

Han 등[16]의 연구에서는 통계적 분석을 통해 일반 사용자와 치팅 사용자의 차이를 확인하였고 룰(rule) 기반의 치팅 사용자 탐지 방법을 제안하였다. 본 논문에서는 사용자 로그 분석을 통한 치팅 사용자 탐지 프레임워크를 제안한다. 치팅 사용자와 일반 사용자의 분류하기 위한 피쳐를 추가하였고 인공 신경망 알고리즘을 적용하여 탐지 성능을 향상시켰다.

3. 방법론

FPS 게임에서 사용자가 치팅 행위를 할 경우 사용자의 게임 플레이에 영향을 미쳐 이전보다 향상된 실력을 발휘하게 되고 일반 사용자와는 다른 행동 패턴이 나타나게 된다. 본 논문에서는 게임 로그 분석을 통해 일반 사용자와 치팅 사용자의 특징을 분석하고 두 사용자 그룹의 차이점을 이용해 치팅 사용자를 탐지하는 프레임워크를 제안한다. 제안하는 프레임워크는 크게 4단계로 구성되며 [Fig. 2]는 제안하는 프레임워크의 전반적인 개요를 보여준다.



[Fig. 2] Overview of Cheating User Detection Framework

게임 로그 수집 단계에서는 사용자의 게임 플레이 정보와 클라이언트 기반의 보안 솔루션에 의해 탐지된 치팅 탐지 목록을 수집하고 데이터베이스에 저장하게 된다.

데이터 전처리 단계에서는 데이터 가공 작업을 진행하게 된다. 수집된 원본 데이터를 정규화하여 분석 가능한 형태의 데이터 형식으로 변환하는 작업을 수행한다. 그리고 치팅 탐지 로그를 이용해 치팅 사용자 로그에 태그(tag)를 붙여 일반 사용자와 치팅 사용자의 로그를 구분한다.

게임 로그 분석 단계에서는 실제 게임 서비스에 적용 가능한 피쳐를 중심으로 일반 사용자와 치팅 사용자에 대한 비교 분석을 수행하고 치팅 사용자와 일반 사용자의 특징이 뚜렷하게 나타나는 피쳐를 선택하는 작업을 수행한다.

탐지 모델 생성 단계에서는 모델 학습에 사용할 데이터를 샘플링하는 작업을 진행한다. 모델 학습에 사용할 학습 데이터와 모델 검증에 사용할 테스트 데이터를 기간 별로 분할하고 학습 데이터의 경우 치팅 사용자와 일반 사용자의 비대칭적인 비율로 인해 모델 학습 과정에서 학습률이 떨어질 수 있으므로 랜덤 샘플링(random sampling)을 이용해 일반 사용자와 치팅 사용자의 데이터의 비율을 균등하게 샘플링한다. 최종적으로 샘플링한 학습 데이터에 인공 신경망 알고리즘인 MultiLayer Perceptron을 적용해 치팅 사용자 탐지 모델을 생성한다. MultiLayer Perceptron은 인공 신경망 알고리즘에서 가장 널리 사용되고 있는 알고리즘으로 일반적으로 다른 Classification 알고리즘에 비해 우수한 성능을 발휘하는 것으로 알려져 있다. 학습을 통해 생성된 치팅 사용자 모델은 테스트 데이터를 이용해 치팅 사용자 탐지 성능을 평가한다.

4. 실 험

4.1 데이터 셋

국내 게임 개발 업체인 [1]제페토에서 개발한 포인트 블랭크의 브라질 데이터를 사용하였다. 포인트 블랭크는 2013년 브라질에서 동시접속자 5만명을 달성하며 FPS 게임순위 1위에 올랐었고 현재 전 세계 70개국에서 서비스 중이다[17]. 본 논문에서는 2014년 2월 14일부터 2월 28일까지 15일간의 데이터를 사용하였으며 해당 기간 동안 541,884명의 고유한 사용자가 총 49,279,223건의 게임을 플레이했다.

4.2 데이터 전처리

수집된 원본 데이터를 실험에 적합한 형태로 변환하기 위해 데이터 전처리 작업을 진행하였다.

일부 사용자의 경우 게임 플레이 횟수가 적어 통계적 분석에 어려움이 있었다. 본 논문에서는 휴리스틱하게 임계값을 설정하였고 과거 게임 플레이 횟수가 10건 이하이거나 당일 게임 플레이시간이 10분 이하인 사용자는 실험 대상에서 제외하였다.

1) 제페토 홈페이지 주소: http://www.zepetto.com/

[Table 1] Description of features

Feature	Description	Formula
KillRatio	The ratio that a user kills his opponents in games in a day. hypothesis: KillRatio of a cheater is higher than that of a normal user.	$\frac{Kill}{Kill+Death}$
HeadshotRatio	The ratio that a user shoots in the head of opponents in games in a day. hypothesis: HeadshotRatio of a cheater is higher than that of a normal user.	$\frac{Headshot}{Kill}$
WinRatio	The ratio that a user wins in games in a day. hypothesis: WinRatio of a cheater is higher than that of a normal user.	$\frac{Win}{Win+Lose}$
AvgKillInterval	The average time interval that a user kills his opponents in a day. hypothesis: AvgKillInterval of a cheater is less than that of a normal user.	$\frac{GamePlayTime}{Kill}$
GamePlayNum	The total number of times that a user plays games in a day. hypothesis: The degree of game immersion of a cheater is higher than that of a normal user.	$Nmber\ of\ GamePlay$
AvgGamePlay Time	The average time that a user plays in games in a day. hypothesis: AvgGamePlayTime of a cheater is shorter than that of a normal user.	$\frac{GamePlayTime}{Nmber\ of\ GamePlay}$
IntrusionRatio	The ratio that a user enters ongoing games in a day. hypothesis: IntrusionRatio of a cheater is higher than that of a normal user.	$\frac{Nmber\ of\ Intrusion}{Nmber\ of\ GamePlay}$
KillRatioChange	The differentials between killRatio of a user in a day and Average KillRatio of user. hypothesis: KillRatioChange is greatly increased when a user cheats in game.	$KillRatio - AvgKillRatio$

4.2.1 정규화

사용자마다 게임 플레이 횟수와 시간이 다르기 때문에 원본 데이터의 사용자 플레이 수치를 단순 비교하는 것은 왜곡된 결과를 초래할 수 있다. 이를 막기 위해, 각 사용자 별로 하루 단위의 집계 데이터를 생성하고 정규화 작업을 진행하였다.

도메인 지식을 이용해 8가지 피쳐를 선택하였으며, 각 피쳐를 계산하기 위해 사용하는 데이터가 사용자의 Kill 횟수, 플레이 시간과 같이 FPS 게임에서 일반적으로 서버에 저장되는지를 고려하였다. 이를 통해 다른 종류의 FPS 게임에서도 동일한 피쳐의 추출이 가능하다. [Table 1]은 선정된 피쳐에 대한 설명과 계산식을 보여준다.

전처리가 완료된 테이블의 각 레코드는 사용자가 1일 동안 플레이한 정보의 집계 데이터이며 사용자 ID, 날짜, 8개의 피쳐로 구성된다.

4.2.2 치팅 사용자 태깅

일반 사용자와 치팅 사용자의 데이터를 구분하기 위해 치팅 탐지 목록을 이용해 게임 플레이 로그에 태그를 붙이는 작업을 진행하였다.

게임 회사에서 제공해 준 치팅 로그는 클라이언트 기반의 보안 솔루션에 의해 탐지된 치팅 사용자 목록으로 치팅 행위 사용 여부가 아닌 치팅 프로그램 실행 여부로 탐지된 로그이다. 그리고 일부 사용자는 오탐으로 인해 탐지된 사용자들이 포함되

어있다. 본 연구에서는 실제 치팅을 사용한 활성화된 치팅 사용자를 추출하기 위해 EM 클러스터링 알고리즘을 이용하여 치팅 사용자를 2개의 클러스터로 군집화하였다. 클러스터1은 전체 치팅 사용자의 71%가 군집화 되었으며, 클러스터2는 29%가 군집화되었다. [Table 2]는 치팅 사용자 클러스터들과 일반 사용자 그룹이 피쳐들에 대해 가지는 평균과 표준 편차를 보여준다.

[Table 2] Summary of clusters

Feature	Cheater Cluster1 (71%)	Cheater Cluster2 (29%)	Normal User
KillRatio			
mean	0.715	0.460	0.455
std. dev.	0.105	0.120	0.130
HeadshotRatio			
mean	0.572	0.333	0.340
std. dev	0.244	0.165	0.173
WinRatio			
mean	0.687	0.480	0.507
std. dev	0.164	0.199	0.196
AvgKillInterval			
mean	22.985	74.454	76.136
std. dev	12.485	228.759	170.642
GamePlayNum			
mean	27.234	29.556	23.305
std. dev	21.930	30.978	22.427
AvgGamePlayTime			
mean	255.440	322.056	320.297
std. dev	89.037	151.563	127.781
IntrusionRatio			
mean	0.684	0.539	0.531
std. dev	0.213	0.235	0.236
KillRatioChange			
mean	0.146	-0.070	0.027
std. dev	0.146	0.124	0.106

측정된 통계적 수치를 이용해 두 개의 치팅 사용자 클러스터와 일반사용자 그룹을 비교 분석하였다. 클러스터1은 클러스터2에 비해 사용자의 실력을 의미하는 KillRatio, HeadshotRatio, WinRatio의 평균값이 크게 나타났다. 또한 자신의 평균 KillRatio와 마지막 하루 동안 플레이한 KillRatio의 차이를 나타내는 KillRatioChange도 높게 나타났다. 반면 클러스터2와 일반 사용자 그룹은 8개 피쳐에서 전반적으로 비슷한 수치를 나타낸다.

클러스터 간의 거리를 비교하기 위해 클러스터의 중심 값(centroid)을 이용해 유클리드 거리(Euclidean Distance)를 측정하였다. 유클리드 거리는 다음과 같이 정의 된다.

$p=(p_1,p_2,\ldots,p_n)$, $q=(q_1,q_2,\ldots,q_n)$ 일 때,

$$\text{distance}(p,q) = \sqrt{\sum_{i=1}^{n}(p_i-q_i)^2}$$

치팅 사용자 클러스터 간의 거리는 84.21, 치팅 사용자 클러스터2와 일반 사용자 그룹의 거리는 6.7로 계산되었다.

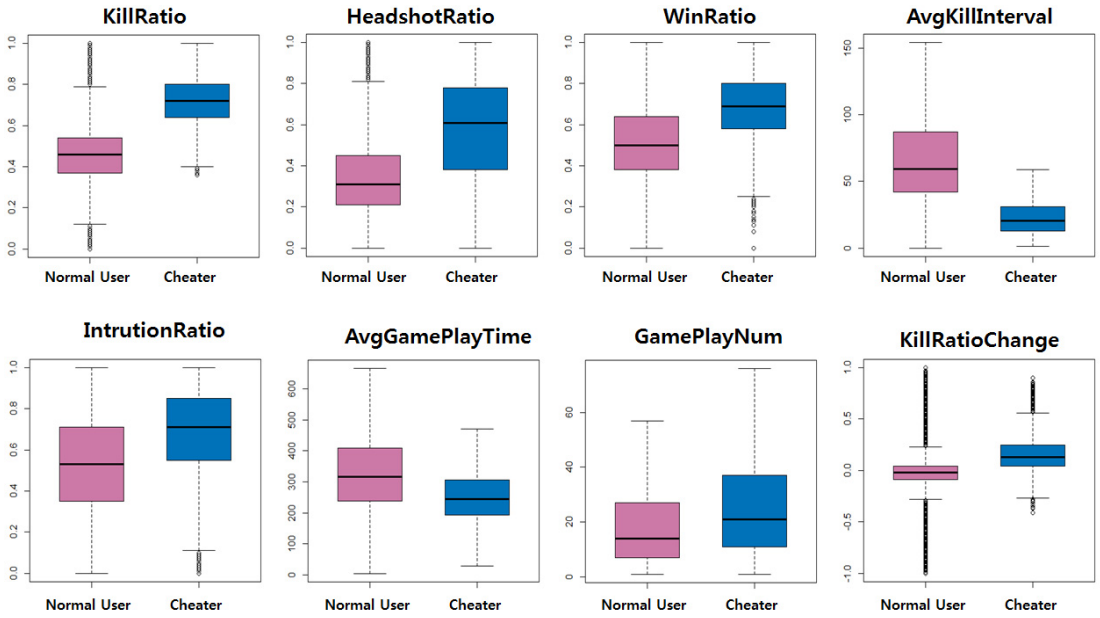
클러스터 간의 통계적 비교와 유클리드 거리 측정을 통해 치팅 사용자 클러스터1을 실제 치팅을 사용한 활성화된 치팅 사용자로 확인하였고 치팅 사용자 클러스터1만을 게임 플레이 로그에 치팅 사용자로 태깅(tagging)하여 실험을 진행하였다.

4.3 게임 로그 분석

4.3.1 데이터 탐색

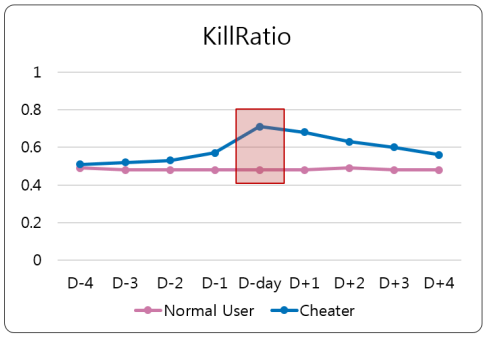
일반 사용자와 활성화된 치팅 사용자의 차이를 확인하기 위해 두 사용자 그룹 간의 비교 분석을 수행하였다. [Fig. 3]은 일반 사용자와 활성화된 치팅 사용자의 8가지 피쳐에 대한 박스플롯(Boxplot)을 보여준다. 박스플롯은 자료의 측정값들이 어떤 모양으로 분포되어 있는지와 데이터의 이상치의 위치를 쉽게 파악할 수 있다.

활성화된 치팅 사용자는 FPS 게임에서 실력을 나타내는 측정 지표로 많이 사용되는 KillRatio, HeadshotRatio, WinRatio 피쳐에서 일반 사용자보다 큰 값에 분포되어 있는 것을 확인할 수 있다. 특히 KillRatio의 경우 두 사용자 그룹의 제1사분



[Fig. 3] Features of normal user and cheater

위수와 제3사분위수 사이 구간이 완전히 분리되어 있으며 이는 두 사용자 그룹 간의 차이가 뚜렷하게 나타남을 보여준다. AvgKillInterval은 활성화된 치팅 사용자가 일반 사용자보다 작은 값에 분포하게 되는데 치팅 사용자가 치팅의 이점을 토대로 두려움 없이 게임 내에서 활발히 움직여 빠르게 킬을 하는 것으로 추측된다. IntrusionRatio는 게임이 진행 중인 방에 입장한 비율로, 활성화된 치팅 사용자의 난입비율이 더 높게 나타났다.



[Fig. 4] KillRatio of Normal User and Cheater in time-series

KillRatioChange는 사용자의 하루 동안 KillRatio와 과거 자신의 평균 KillRatio의 차이로 양수 값이 나올 경우 실력이 향상된 것으로 볼 수 있다. [Fig. 4]는 일반 사용자와 활성화된 치팅 사용자의 시간에 따른 KillRatio의 변화를 보여준다. 일반 사용자는 치팅을 하지 않으므로 2014년 2월 14일부터 22일까지 9일 동안에 평균 KillRatio를 표시하였고 활성화된 치팅 사용자의 경우 치팅으로 탐지되기 전 4일과 치팅으로 탐지된 이후 4일 동안에 평균 KillRatio를 표시하였다.

일반 사용자는 9일 동안 KillRatio의 변동이 거의 없지만 활성화된 치팅 사용자의 경우 치팅을 사용하는 날 KillRatio가 급격하게 증가하는 것을 볼 수 있다. 치팅은 지속적으로 사용되는 경향이 있어 최초 치팅 탐지일 이후 KillRatio가 완만하게 감소하는 것을 볼 수 있다.

KillRatio의 급격한 증가로 인해 활성화된 치팅 사용자의 KillRatioChange가 높게 나타났으며, 이 피쳐는 사용자의 과거 KillRatio와의 유사성을 나타내며 높은 실력을 가진 일반 사용자와 치팅 사용자를 구분하는데 효과적이다.

AvgGamePlayTime, GamePlayNum의 경우 일반 사용자와 활성화된 치팅 사용자의 평균 차이가 크지 않고 박스플롯을 통해 데이터 분포를 확인한 결과, 두 사용자 그룹의 제1사분위수와 제3사분위수 사이 구간이 50%이상 중첩되어 있음을 확인하였다. 이를 토대로 두 가지 피쳐는 치팅 사용자 탐지에 부적합하다고 판단하였다.

4.3.2 피쳐 선택

데이터마이닝 알고리즘의 경우 데이터의 차원이 증가할수록 이로 인한 연산량과 시간도 기하급수적으로 증가하게 되므로 학습에 불필요한 피쳐는 제거하는 것이 타당하다. 본 논문에서는 8개 피쳐 중 일반 사용자와 활성화된 치팅 사용자의 특성이 잘 나타나는 6개(KillRatio, HeadshotRatio, WinRatio, AvgKillInterval, IntrusionRatio, KillRatioChange)의 피쳐를 모델 학습에 사용할 피쳐로 선택하였다.

4.4 탐지 모델 생성

4.4.1 샘플링(sampling)

활성화된 치팅 사용자 탐지 모델 생성과 검증을 위해 전처리된 데이터를 학습 데이터와 테스트 데이터로 분할하였다. 학습 데이터는 모델 학습 과정에 사용되며 2014년 2월 14일부터 20일까지 7일 동안에 데이터를 사용하였고 테스트 데이터는 생성한 모델 검증에 사용되며 2014년 2월 21일부터 28일까지 8일 동안에 데이터를 사용하였다.

학습 데이터의 클래스 비율이 비대칭일 경우 모델 학습 성능을 떨어뜨리므로, undersampling 알고리즘을 이용해 샘플을 추출하여 일반 사용자와 활성화된 치팅 사용자의 로그 비율을 50:50으로 조정하였다. 이를 통해 46,820개의 인스턴스(instance)를 가지는 학습 데이터와 1,289,425개의 인스턴스를 가지는 테스트 데이터를 생성하였다.

4.4.2 탐지 모델 학습

치팅 사용자 탐지 모델을 생성하기 위해 인공 신경망 알고리즘인 MultiLayer Perceptron을 사용하였다. 인공 신경망 알고리즘은 인간의 두뇌의 신경세포를 모방한 개념으로, 노드(node)와 링크(link)로 구성되며 노드를 계층(layer) 별로 구성하여 링크에 수정 가능한 가중치를 부여하고 반복적인 학습을 통해 모델을 생성한다.

학습 데이터에 인공 신경망 알고리즘을 적용해 치팅 사용자 탐지 모델을 학습하였고 사용자 분석을 통해 선택된 6개 피쳐만을 사용하였다. 생성된 치팅 사용자 탐지 모델은 각 사용자가 특정 날짜에 치팅을 사용했는지 여부를 탐지하게 된다.

탐지 모델 학습 및 검증은 CPU 3.4GHz(8코어), RAM 16G 성능의 PC에서 진행하였으며, 학습 데이터를 이용한 모델 생성에는 44.29초의 시간이 소요되었고 테스트 데이터를 이용한 모델 검증에는 3초의 시간이 소요되었다.

5. 실험 결과

테스트 데이터를 이용해 생성된 치팅 사용자 탐지 모델에 대한 성능 평가를 수행하였다. 실험 결과 분석을 위해 데이터 마이닝에서 이진 분류 모델 성능 평가에 대표적으로 사용하는 정밀도(precision), 재현율(recall), 정확도(accuracy)의 3가지 평가 지표를 사용하였다. 각 평가 지표는 아래와 같이 정의된다.

$$\text{Precision} = \frac{TP}{TP + FP}$$

$$\text{Recall} = \frac{TP}{TP + FN}$$

$$\text{Accuracy} = \frac{TP + TN}{Total}$$

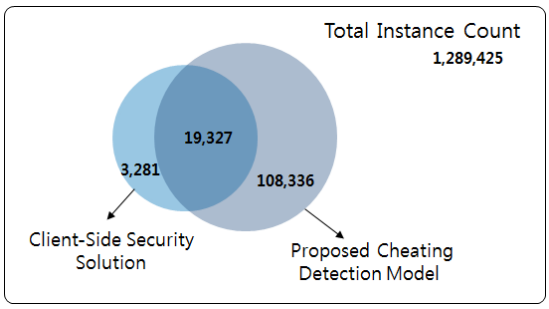
TP: True Positive TN: True Negative
FP: False Positive FN: False Negative

정밀도는 탐지 모델에 의해 탐지된 치팅 사용자가 실제 치팅 사용자일 비율을 의미하고 재현율은 게임 회사에 의해 탐지된 치팅 사용자가 탐지 모델에 의해 탐지되는 비율을 나타낸다. 그리고 정확도는 전체 데이터에 대해 탐지 모델이 정확하게 예측한 비율을 의미한다.

[Table 3] Evaluation of cheater detection model

	Normal User	Cheater
Precision	0.997	0.151
Recall	0.914	0.855
Accuracy	91.34%	

[Table 3]은 탐지 모델의 성능을 평가한 결과를 보여준다. 치팅 사용자 탐지 모델은 전체 예측에 대해 91.34%의 정확도를 나타냈다. 일반 사용자에 대한 예측의 경우 정밀도와 재현율이 모두 0.9 이상으로 높게 나왔지만 치팅 사용자에 대한 예측의 경우 정밀도가 0.151로 낮게 나왔다. 이는 제안하는 치팅 사용자 탐지 모델이 추가적으로 탐지한 치팅 사용자 목록이 성능 평가 정답지로 사용한 게임 회사의 치팅 사용자 로그에 존재하지 않기 때문이다. 클라이언트 단의 보안 솔루션은 시그니처 기반의 탐지 방법을 사용해 알려지지 않은 치팅 프로그램에 대한 탐지가 어렵지만 제안하는 치팅 탐지 모델의 경우 두 사용자 그룹의 차이를 이용해 탐지를 수행하므로 치팅 프로그램 종류에 상관없이 탐지가 가능하다.



[Fig. 5] Result of cheater detection

[Fig. 5]는 치팅 사용자 예측 결과를 보여준다. 제안하는 치팅 사용자 탐지 모델은 클라이언트 단의 보안 솔루션이 탐지한 치팅 사용자의 85.5%를 탐지하였으며 추가적으로 108,336건의 치팅을 탐지하였다.

6. 결 론

본 논문에서는 서버 단에서 사용자 로그 분석을 통해 치팅 사용자를 탐지하는 프레임워크를 제안하였다.

FPS 게임에서 치팅 행위는 사용자에게 빠른 반응 속도, 다른 사용자의 위치 확인 등의 다양한 이점을 제공하므로 일반 사용자와 치팅 사용자의 게임 플레이에 차이가 발생하게 된다. 우리는 실제 서비스되고 있는 FPS 게임의 로그를 이용해 두 사용자 그룹에 대한 비교 분석을 진행하였고 다음과 같은 사실을 확인하였다. 치팅 사용자는 일반 사용자에 비해 게임 실력을 나타내는 지표인 KillRatio, HeadshotRatio, WinRatio가 높게 나타났으며 KillInterval은 일반 사용자에 비해 낮고 진행중인 게임에 자주 난입하는 경향이 강한 것으로 확인되었다. 그리고 치팅 사용자가 과거 자신의 평균 KillRatio와의 변동량을 나타내는 KillRatioChange가 높게 나타는 것으로 확인되었으며 이 피쳐는 실력이 뛰어난 일반 사용자와 치팅 사용자를 분류하는데 효과적이다.

분석된 내용을 토대로 치팅 사용자 탐지에 적합한 6개의 피쳐를 선정하였다. 또한 피쳐 선택 과정에서 해당 피쳐를 생성하는 데이터가 FPS 게임에서 일반적으로 저장되는 로그인지를 고려하였으며 이를 통해 다른 FPS 게임에서도 별도의 시스템 조작 없이 해당 피쳐의 사용이 가능하다.

샘플링된 학습 데이터에 인공 신경망 알고리즘인 MultiLayer Perceptron을 적용하여 치팅 사용자 탐지 모델을 학습하였다. 생성된 치팅 사용자 탐지 모델은 테스트 데이터를 이용해 검증하였다.

전체 예측에 대해 91.34%의 높은 정확성을 나타냈으며 클라이언트 단의 보안 솔루션에서 탐지하지 못했던 108,336명의 사용자를 추가적인 치팅 사용자로 탐지하였다.

그리고 서버 단에서 치팅 사용자 탐지를 수행하여 클라이언트 단에서의 문제점을 극복하였다. 이러한 서버 단에서의 탐지 방법은 사용자의 게임 진행에 영향을 주지 않아 높은 사용자 편리성(usability)을 보장하며 사용자 특징을 이용해 치팅 사용자를 탐지하므로 알려지지 않은 치팅 프로그램에 대해 효율적인 탐지가 가능하다. 또한 사용자 제재 규모와 제재시기를 자유롭게 선택할 수 있는 장점을 가지게 된다. 본 논문에서 제안하는 탐지 방법은 하루 동안 사용자 플레이에 대한 집계 데이터를 이용해 치팅 유무를 판단하기 때문에 최소 하루 전의 사용자 플레이에 대한 사후 분석이 가능하다. 하지만 한 번 치팅을 한 사용자는 지속적으로 치팅을 사용할 확률이 높으므로 향후 발생할 치팅으로 인한 피해를 예방할 수 있다.

7. 향후 연구

향후 연구에서는 게임 플레이 로그 이외에 로그인 관련 로그, 아이템 거래 관련 로그, 소셜 관련 로그 등의 다양한 사용자 로그 분석을 통해 일반 사용자와 치팅 사용자의 차이를 추가적으로 확인할 것이다. 추가적으로 발견된 두 사용자 간의 차이점은 치팅 사용자 탐지 성능 향상에 도움이 될 것으로 예상된다.

그리고 제안하는 탐지 모델에 의해 추가적으로 탐지된 치팅 사용자에 대한 검증을 수행할 것이다. 실험 기간 이후의 치팅 로그를 이용해 추가적으로 탐지된 치팅 사용자에 대해 추적 조사를 진행하고 실력이 뛰어난 일반 사용자와 치팅 사용자와의 비교 분석을 통해 검증을 수행할 것이다.

ACKNOWLEDGMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Planning(2014R1A1A1006228). In addition, this research was supported by the MSIP(Ministry of Science, ICT & Future Planning), Korea, under the “The Types of employment contract to support master‘s degree in Information Security” supervised by the KISA(Korea Internet Security Agency).

REFERENCES

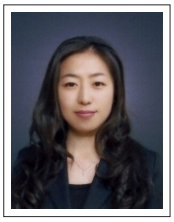
[1] Korea Creative Content Agency (2014 White Paper on Korea Games), http://www.kocca.kr
[2] Im, Sung-Jin, and Lee, Dae-Hyun, “A Study on Cheating Patterns in Online FPS Games and their Countermeasures: By the Case of Point Blank in Indonesia.”, Journal of Korea Game Society, 11.2, 81-91, 2011.
[3] Kang, Ah Reum, et al., “Online game bot detection based on party-play log analysis.”, Computers & Mathematics with Applications, 65.9, 1384-1395, 2013.
[4] Alayed, Hashem, et al., “Behavioral-based cheating detection in online first person shooters using machine learning techniques.”, Computational Intelligence in Games (CIG), 2013 IEEE Conference on. IEEE, 1-8, 2013.
[5] Yoo, Dong-Young, et al., “A Study for Effectiveness of Preliminary Security Assessment on Online Game Service Domain.”, Journal of the Korea Society of IT Services, 10.2, 293-308, 2011.
[6] Yu, Su-Yang, et al., “A statistical aimbot detection method for online FPS games.”, Neural Networks (IJCNN), The 2012 International Joint Conference on. IEEE, 1-8, 2012.
[7] Woo, Kyungmoon, et al., “What can free money tell us on the virtual black market?.”, A

CM SIGCOMM Computer Communication Review, 41.4, 392-393, 2011.
[8] Thawonmas, Ruck, et al., "Detection of MMORPG bots based on behavior analysis.", Proceedings of the 2008 International Conference on Advances in Computer Entertainment Technology. ACM, 91-94, 2008.
[9] Chen, Kuan-Ta, and Hong, Li-Wen, "User identification based on game-play activity patterns.", Proceedings of the 6th ACM SIGCOMM workshop on Network and system support for games. ACM, 7-12, 2007.
[10] van Kesteren, Marlieke, et al., "A step in the right direction: Botdetection in MMORPGs using movement analysis.", Proceedings of the 21st Belgian-Dutch Conference on Artificial Intelligence. 2009.
[11] Chen, Kuan-Ta, et al., "Identifying MMORPG bots: A traffic analysis approach.", EURASIP Journal on Advances in Signal Processing 2009, 3, 2009.
[12] Kim, Hyungil, et al., "Detection of auto programs for MMORPGs.", AI 2005: Advances in Artificial Intelligence. Springer Berlin Heidelberg, 1281-1284, 2005.
[13] Yampolskiy, Roman V., and Govindaraju, Venu, "Embedded noninteractive continuous bot detection.", Computers in Entertainment (CIE), 5.4, 7, 2008.
[14] Chen, Kuan-Ta, et al., "Game bot identification based on manifold learning.", Proceedings of the 7th ACM SIGCOMM Workshop on Network and System Support for Games. ACM, 21-26, 2008.
[15] Galli, Luca, et al., "A cheating detection framework for unreal tournament III: a machine learning approach.", Computational Intelligence and Games (CIG), 2011 IEEE Conference on. IEEE, 266-272, 2011.
[16] Han, Mee Lan, et al., "Online Game Bot Detection in FPS Game.", Proceedings of the 18th Asia Pacific Symposium on Intelligent and Evolutionary Systems-Volume 2. Springer International Publishing, 479-491, 2015.
[17] Point Blank FPS Game Information, http://www.fps-pb.com/

박 정 규(Park, Jung Kyu)

2012년 2월 백석대학교 정보보호대학과 졸업
2013년 3월-현재 고려대학교 정보보호대학원 석사과정

관심분야 : 온라인게임 보안, 데이터마이닝, 리버스 엔지니어링



한 미 란(Han, Mee Ran)

2002년 2월 동덕여자대학교 컴퓨터공학 학사 졸업
2004년 5월-2012년 3월 NEXON 해외사업 개발본부
2014년 8월 고려대학교 정보보호대학원 석사 졸업
2014년 9월-현재 고려대학교 정보보호대학원 박사과정

관심분야 : 온라인게임 보안, 데이터마이닝, 보안 시각화

김 휘 강(Kim, Huy Kang)

1998년 2월 KAIST 산업경영학과 학사 졸업
2000년 2월 KAIST 산업공학과 석사 졸업
2009년 2월 KAIST 산업및시스템공학과 박사 졸업
2004년 5월-2010년 2월 엔씨소프트 정보보안실장, Technical Director
2010년 3월-현재 고려대학교 정보보호대학원 부교수

관심분야 : 온라인게임 보안, 네트워크 보안, 네트워크 포렌식