情報保護學會論文誌
第 22 卷 第 3 號, 2012. 6

연결패턴 정보 분석을 통한 온라인 게임 내 불량사용자 그룹 탐지에 관한 연구*

서 동 남,[1†] 우 지 영,[1] 우 경 문,[2] 김 종 권,[2] 김 휘 강[1‡]
[1]고려대학교, [2]서울대학교

Detecting gold-farmers' group in MMORPG by analyzing connection pattern*

Dongnam Seo,[1†] Jiyoung Woo,[1] Kyung-moon Woo,[2] Chong-kwon Kim,[2] Huy Kang Kim[1‡]
[1]Korea University, [2]Seoul National University

요 약

온라인 게임 산업이 성장함에 따라 온라인 게임 보안 이슈는 증가하고 있다. 특히 게임내의 사이버재화를 현금으로 바꾸는 행위인 현금거래(RMT; Real Money Trade)는 탈세나 돈세탁등과 같은 실물경제의 범죄활동과 연관되면서 국내를 비롯한 여러 나라에서 민감한 문제로 떠오르고 있다. 이러한 현금거래는 작업장이라고 불리는 전문적인 불량사용자 조직에 의해 이루어진다. 온라인 게임 사업자들은 이러한 작업장을 탐지하기 위하여 게임 bot 탐지 알고리즘을 이용해 각각의 bot 사용자를 탐지하고 그들의 계정과 IP 주소를 차단하고 있다. 하지만 게임 bot 탐지 알고리즘은 작업장의 일부분만 탐지가 가능하여 큰 효과를 거두기 어렵고, IP 주소 차단 역시 IP 변조나 가상 사설망 기술을 이용하여 쉽게 우회 가능하다는 문제점을 가진다. 본 논문에서는 온라인게임 서비스를 이용하는 사용자들의 연결패턴 정보에 데이터마이닝 기법을 적용하여, 작업장 그룹 내 불량사용자 군집을 탐지할 수 있는 모델을 제안한다. 제안한 모델을 활용하여 IP 변조나 VPN 기술을 통한 우회접속 역시 탐지할 수 있다. 국내 최대 온라인 게임의 실제 데이터를 샘플로 하여 수행결과를 도출하였고, 본 논문에서 제시한 기법을 이용한 결과를 실제 차단 리스트와 비교하여 본 결과, 효율적으로 작업장을 탐지해 낼 수 있음을 확인할 수 있었다.

ABSTRACT

Security issues in online games are increasing as the online game industry grows. Real money trading (RMT) by online game users has become a security issue in several countries including Korea because RMT is related to criminal activities such as money laundering or tax evasion. RMT-related activities are done by professional work forces, namely gold-farmers, and many of them employ the automated program, bot, to gain cyber asset in a quick and efficient way. Online game companies try to prevent the activities of gold-farmers using game bots detection algorithm and block their accounts or IP addresses. However, game bot detection algorithm can detect a part of gold-farmer's network and IP address blocking also can be detoured easily by using the virtual private server or IP spoofing.

In this paper, we propose a method to detect gold-farmer groups by analyzing their connection patterns to the online game servers, particularly information on their routing and source locations. We verified that the proposed method can reveal gold-farmers' group effectively by analyzing real data from the famous MMORPG.

Keywords: MMORPG, gold-farmer, Data mining, VPN, connection pattern

접수일(2012년 1월 16일), 수정일(2012년 2월 28일), 게재확정일(2012년 3월 13일)
* 본 연구는 지식경제부 및 정보통신산업진흥원의 "대학 IT 연구센터 육성·지원사업"의 연구결과로 수행되었음 (NIPA-2012-H0301-12-3007)
† 주저자, deepgust@hksecurity.net
‡ 교신저자, cenda@korea.ac.kr

I. 서 론

온라인 게임 산업이 발전함에 따라 온라인 게임 보안 이슈는 더욱 증가하고 있다. 특히 현금거래는 현재 온라인 게임의 가장 큰 문제 중의 하나이다. 현금거래는 게임내의 재화를 수집하여 그것을 현실 세계의 재화로 바꾸는 행위이다. 이러한 현금거래는 온라인 게임내의 경제 균형을 망치는 행위로 온라인 게임 서비스 사업자에게도 중요한 문제이다. 현금거래는 돈세탁이나 탈세 등과 같은 범죄활동과 연관되고 있으며[1], 2010년 2월 기준, 가상재화의 거래시장 규모는 6억 달러 이상으로 연간 40% 이상 성장하고 있다[2]. 아이템베이, 아이템매니아 등 국내 현금거래 사이트에서 거래된 자료를 집계한 내용에 따르면, 국내 게임아이템 시장의 규모는 2009년 1조 5천억을 넘었으며 당시 온라인게임시장 규모 3조 7천억의 약 41%, 2010년에는 2조에 근접하는 거대한 시장을 이루었다. 또한 리서치회사인 Park Associates에 의해 2010년에 수행된 조사에 따르면 전 세계적으로 온라인게임 아이템 구입을 통해 발생될 수익은 2015년까지 60억 달러(한화 약 6조 7천억)가 될 것으로 예상되고 있다[3].

대부분의 현금거래는 골드파밍(gold farming)에 의해 이루어진다. 골드파밍이란 작업장으로 불리는 전문적인 집단이, 게임 내에서 반복적이고 단순한 경제 이득을 취할 수 있는 행위를 자동화하여 게임내의 가상 재화를 축적하고 그 가상 재화를 현금으로 바꾸기 직전까지의 일련의 행위를 말한다. 이러한 골드파밍 활동은 게임내의 경제 및 활동 균형을 파괴하고 정상적인 사용자의 게임 내 활동을 방해하기 때문에, 결국에는 정상적인 사용자들이 게임에 흥미를 잃고, 상대적인 박탈감을 느끼며, 게임 내 경쟁력을 상실하게 되어 그 게임을 떠나게 할 수 있다.

골드파밍의 반복적인 행위는 과거에는 사람이 직접 행하였지만 최근에는 봇(bot) 또는 game bot(이하 bot) 이라고 불리는 프로그램이 자동으로 수행해 주고 있다. 봇은 로봇(robot)에서 유래한 용어로, 온라인 게임에서의 봇은 사람의 조작 없이 자동으로 게임을 수행할 수 있게 해주는 프로그램을 의미하며, 게임 내에서 몬스터들을 인식하여 사냥하고, 게임 내의 재화를 획득, 그에 대한 판매와 처분까지 대신해주고 있다. 이에 따라 작업장에서는 인건비를 줄이고, 한 대의 PC에서 다수의 클라이언트를 실행시키면서 효율을 높여 그 규모가 더 커져가고 있다. 일반적으로 게임 클라이언트를 구동하면서 게임 봇 프로그램이 같이 동작하는 in game bot의 형태가 대부분이나, 일부 게임은 내부 알고리즘 및 통신 프로토콜까지 파악되어 클라이언트 프로그램 없이도 게임을 실행하고 골드파밍 활동을 할 수 있는 out of game bot 까지 개발되어 있어 그 피해는 더욱 심각하다.

온라인 게임 서비스 사업자는 이러한 골드파밍 활동을 예방하기 위해 봇을 탐지하고, 이러한 불량 사용자들의 계정과 IP 주소를 차단하고 있다. 골드파밍 행위를 많이 일으키는 작업장은 보통 특정 국가에 위치해 있는 경우가 많아서, 온라인 게임 서비스 사업자들은 보통 해당 특정 국가의 IP 대역을 Network 장비에서 전체 차단을 하고 있는 것이 일반적이다. 하지만, 이러한 제재/차단 활동들은 큰 효과를 보지 못하고 있다. IP 주소 기반의 접근 제어는 가상사설망(VPN: Virtual Private Network) 같은 서비스 또는 IP 변조를 통하여 쉽게 우회가 되기 때문에 IP 대역을 기반으로 특정 국가의 IP 주소를 차단하여도 손쉽게 우회가 되고 있어 큰 효과를 보지 못하고 있다. 작업장에서는 게임 계정 매매도 활동도 활발하다. 다른 사람 명의의 계정을 현금을 주고 사들인 뒤, 골드파밍 활동을 하고 있던 계정이 차단을 당했을 때, 손쉽게 여분의 다른 계정 및 캐릭터를 골드파밍에 쓸 수 있기 때문에 계정제재 활동 역시 큰 효과가 있다고 할 수 없는 소모적인 작업이라 할 수 있다. 이렇게 제재당한 계정들은 사이트 탈퇴 후 시간이 지나 관련 정보가 게임회사 서버에서 사라지면 해당 명의로 재가입을 하고, 재가입에 필요한 공인인증서까지 포함하여 파는 경우가 많아 계정 제재 또한 큰 효과를 보기 어렵다[4].

본 연구는 이러한 문제를 해결하기 위해 우회 접속을 시도하는 사용자들을 탐지하고, 전문적으로 골드파밍 활동을 하는 작업장을 탐지하는 방법을 제안한다. 작업장에서 IP 주소 차단으로부터 자신의 정체를 숨기기 위하여 VPN 연결 서비스를 사용한다는 사실을 기반으로, 계정명과 MAC 주소, 라우팅 경로 및 IP 주소의 위치정보를 포함하여 연결패턴을 분석함으로써 일반사용자와 작업장을 분류한다. 이것을 통하여 게임 봇 프로그램을 사용하지 않는 작업장과, 직접적으로 봇을 사용하여 제재의 대상이 되는 계정과 이와 관련된 주변 계정까지 탐지할 수 있는 모델을 제안한다.

II. 관련 연구

봇의 사용으로 인한 부정적인 효과는 다음과 같은

3가지로 분류하고 있다. 첫째, 봇이 무차별적으로 사냥을 하고 다니는 것은 그 위치에서 게임을 즐기는 정상적인 사람들에게 문제가 된다. 즉, 주기적으로 생성(spawning)되는 몬스터들을 봇들이 대부분 사냥을 하게 되므로, 정상적인 게임 사용자들이 사냥을 할 수 없게 된다. 둘째, 봇에 의해서 가치 있는 아이템들이 자동으로 대량생산되어 게임 내 유입되므로, 게임 내 아이템 가치의 인플레이션을 유발하는 등, 게임 내 경제에 영향을 미칠 것이다. 셋째, 현금을 벌기 위해 아이템을 수집하고 그것을 현금으로 팔 목적으로 봇을 사용하는 사람들이 존재하게 된다[5][6].

이처럼 게임 봇은 골드파밍의 원인으로 지목되어 오고 있고, 골드파밍 활동이 주로 게임 봇을 동반하기 때문에 게임 봇 탐지 방법이 작업장을 감지하는데 사용되어 왔다. 최근 연구된 봇 / 치팅에 관련된 연구를 크게 나누면 사용자 행동 기반, 이동경로 기반, 트래픽 기반, HOP (Human Observational Proofs) 기반, CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) 기반의 방법으로 분류할 수 있고, 이 분류는 [표 1]과 같다.

2.1 사용자 행동 기반 기법

사용자 행동 기반 방법은 일반 사용자와 봇의 행동 차이를 이용하는 방법으로, 사용자와 봇의 행동 특징의 차이를 이용하는 방법, 플레이 중 발생하는 유휴 시간 측정 방법, 사용자의 예측 가능한 행동 패턴 활용 방법 및 소셜 네트워크(Social network, Social connection) 분석 방법, 자기유사도(Self-similarity)를 사용하는 방법이 있다.

사용자 행동 빈도 비교 방법은 일반 사용자와 봇의 행동 차이를 이용한다. 봇의 게임 내 행동(Action)의 빈도가 일반 사용자들보다 월등히 높다는 특징을 이용하는데, 행동을 유형별로 분류하고 자동학습모델을 이용하여 빈도에 특이치가 존재하는 캐릭터들을 분류한다[6][7]. 유휴 시간 측정 방법은 일반 사용자의 경우 게임을 플레이하는 중에 아무것도 하지 않고 있는 유휴 시간이 매우 불규칙하게 발생한다는 사실을 이용한 방법이다. 활동·유휴 시간에 대한 분포 및 밀도를 측정하거나 최대 유휴 시간 및 활동 시간의 임계값 설정 후 특이 사용자를 분석하는 방법을 이용한다[8]. 사용자 행동 패턴에 대한 확률적 예측 방법은 일반 사용자의 행동 패턴은 예측할 수 있다는 사실을 전제로 상태 전이라는 것을 표현할 수 있으며, Bayesian 모델에 의해 확률적인 예측도 가능하다는 논리를 바탕으로 한다[9]. 소셜 네트워크 분석 방법은 실제 분석을 통해 캐릭터 간의 거리, 접촉 시간 간격, 접속 시간 등을 기반으로 데이터를 분류한 결과 봇은 사회적인 연결의 수치가 낮다는 사실을 발견하고 이를 이용한 것이다

[표 1] 봇 / 치팅에 관련된 논문 분류

분 류	논 문 명
사용자행동 기반	Online Game Bot Detection Based on Party-Play Log Analysis[5]
	Detection of MMORPG Bots Based on Behavior Analysis[6]
	Mining for Gold Farmers: Automatic Detection of Deviant Players in MMOGS[7]
	User Identification based on Game-Play Activity Patterns[8]
	Detecting Cheaters for Multiplayer Games: Theory, Design and Implementation[9]
	Second Life: a Social Network of Humans and Bots[10]
	Data and Text Mining of Communication Patterns for Game Bot Detection[11]
	Self-similarity based Bot Detection System in MMORPG[12]
	What Can Free Money Tell Us on the Virtual Black Market[13]
	Exploiting MMORPG Log Data toward Efficient RMT Player Detection[14]
이동경로 기반	A step in the right direction: Bot detection in MMORPGs using movement analysis[4]
	Server Side Bot Detection in MMOG[15]
	Detection of Landmarks for Clustering of Online-Game Players[16]
트래픽 기반	Identifying MMORPG: Bots A Traffic Analysis Approach[17]
	How to deal with BOT scum in MMORPGs[18]
HOP 기반	Battle of Botcraft: Fighting Bots in Online Games with Human Observational Proofs[19]
	Detection of Auto Programs for MMORPGs[20]
CAPTCHA	Preventing Bots from Playing Online Games[21]
	Embedded Non-interactive Continuous Bot Detection[22]

[10]. 또 다른 소셜 네트워크 분석방법은 사용자 간의 채팅을 이용하는 것이다. 사람은 어떠한 질문에 자신의 생각을 담아서 이야기할 수 있기 때문에 채팅이 매우 자유로운 반면, 봇은 프로그래밍에 의해 만들어지는 패턴으로밖에 대화를 할 수 없으므로 독특하고 비정상적인 채팅 패턴을 보인다는 점을 이용하였다[11]. 자기유사도를 사용하는 방법은 봇과 사람의 반복행동 빈도 차이를 이용한다. 봇은 동일한 행동을 반복하기 때문에 자기유사도가 높고, 일반 플레이어는 여러 가지 행위를 하기 때문에 자기유사도가 낮음을 사용하여 봇과 사람을 구분하였다[12].

이런 사용자 행동 기반 방법들은 사람과 봇의 행동 패턴과 게임 플레이 목적이 명확하게 다르므로 정확도와 탐지율은 높은 편이며, 제재시점과 규모를 통제함으로써 봇 개발자에게 탐지 규칙이 잘 노출되지 않도록 조절할 수 있다. 그러나 게임 내부적으로 반복 수행하는 퀘스트와 같은 시스템이 존재하는 게임에서는 적합하지 않을 수 있다. 데이터의 연산량, 예외 처리 등 처리할 분량이 많고 정확도를 높이기 위해 필요한 특징값들이 많아질수록 많은 시스템 자원이 필요하다. 행동 빈도 비교는 어떤 행동을 정의할 것인가 하는 문제도 수반한다. 또한, 해당 게임을 플레이하는 사용자들의 평균적인 행동 패턴 등에 대한 깊은 이해가 필요하다.

2.2 이동경로 기반 방법

이동경로 기반 탐지 방법은 사용자 행동 기반의 방법과 함께 제재 시점과 규모를 원하는 대로 통제할 수 있다는 점에서 다른 방법들과 구별된다. 일반 사용자와 봇의 이동경로는 다를 것이라는 전제하에 출발한다. 이동경로 기반의 탐지 방법은 크게 좌표 단위 분석 방법과 지역 단위 분석 방법이 있다.

좌표 단위 분석 방법은 다음과 같은 예로 설명할 수 있다. 만약 어떤 캐릭터가 같은 장소에서 출발하여 같은 도착지로 간다고 가정한다. 이런 경우 일반적인 사용자라면 계속 같은 곳으로 이동하려고 노력해도 그 이동경로는 정확할 수 없을 것이다. 그러나 봇은 프로그램이기 때문에 그것이 가능하며 오히려 사람처럼 매번 다른 좌표를 통하여 이동하는 것이 더 힘들 수 있다. 좌표 단위 분석 방법은 바로 이와 같은 가정에서 출발한다[6]. 이 방법은 매우 높은 정확도를 가진다고 할 수 있으나 최근의 봇들은 경로이동에 있어서도 임의성을 가지도록 구성되고 있으므로 탐지하지 못하는 경우가 발생할 수 있다.

지역 단위 분석 방법은 세밀한 좌표단위 분석과는 차이가 있다. 지역 단위 분석은 특정한 지점들을 설정하여, 한 지역에서 다른 지역으로 이동할 때 해당 지점 중 어느 곳을 통하여 이동하는지를 파악 후 탐지하는 방법이다[15][16]. 이 방법은 위의 좌표 분석 방법보다 임의성을 가지도록 구성되고 있는 봇 프로그램에 대해서 유연성을 갖지만, 게임에 익숙하지 않아 맵(Map)을 잘 모르는 사용자나 신규 맵의 경우를 고려해야 한다. 또한, 일반 사용자의 경우에도, 게임을 오래하게 되면 자신만의 플레이 스타일이 생기게 되는데 이때, 일반 사용자임에도 불구하고, 자신이 익숙해진 경로만으로 이동하여 계속 같은 패턴으로 탐지될 수 있다. 이러한 사용자들의 이동패턴의 경우 봇의 이동패턴과 유사하게 보일 수 있다는 점을 고려해야 할 것이다.

이동경로 기반 탐지 방법은 로그를 통하여 각 캐릭터의 이동경로를 추출하는 방법을 사용한다. 분석이 서버 측에서 이루어지기 때문에 사용자들의 게임 플레이에 영향을 미치지 않는다는 장점이 있다. 하지만 최근의 MMORPG의 경우 Seamless Map이라고 알려져 있는 통합되어 있는 맵을 사용함으로써 그 규모가 매우 크기 때문에 전체적인 분석을 시도하였을 때 분석속도가 매우 느려지게 된다. 따라서 주요한 사냥 지점과 같은 특정한 지점에 대해서만 분석을 진행하여야 한다. 또, 이동경로 기반의 방법은 맵의 규모와 사용자의 이동경향에 따라 처리할 데이터의 분량이 많아지기 때문에 데이터 처리의 규모를 잡기 어려울 수 있다. 뿐만 아니라 맵을 잘 모르는 초보자의 이동경로와 숙련자의 이동경로에 차이가 있을 수 있으며, 사람들이 익숙하지 못한 신규 맵인지의 여부도 변수가 될 수 있다. 최근에는 봇의 경우, 일반 사용자와 비슷하게 이동할 수 있게 발전하여 탐지 정확도는 그리 높지 않은 편이다.

2.3 네트워크 트래픽 기반 방법

네트워크 트래픽에 기반을 둔 탐지 방법은 서버나 클라이언트에 별도의 수정 없이 사용할 수 있다. CAPTCHA를 활용한 방법과 함께 일반적으로 실시간 대응을 위주로 하며, OOG 봇의 대응에 특히 유리하다. 트래픽 헤더의 특성치를 연산하는 방법이므로 상대적으로 분석에 많은 연산을 필요로 하지 않는다. 또한 분석을 위해 많은 데이터를 계속 가지고 있지 않

아도 되므로 필요한 자원이 다른 방법에 비해서는 적은 편이다.

네트워크 트래픽 기반 방법은 네트워크 트래픽이 발생하면, 반응상의 특이점을 발견하여 대응하는 방식을 취한다. 예를 들어 봇의 경우, 사람과는 다르게 패킷의 도착 시간 간격이 일정하고, 빠르며, 그 크기가 크지 않을 것이라고 가정한다. 명령 패킷의 타이밍, 트래픽의 폭발성과 그 추세 및 규모, 네트워크 상태에 대한 반응을 이용한다[17]. 봇으로부터의 응답 시간이 짧다는 특징을 이용한 명령 패킷의 타이밍 확인 방법, 봇의 경우 메인 루트가 반복될 때마다 동일한 수의 패킷을 보내게 된다는 특징을 이용한 트래픽의 폭발성 확인 방법, 사람의 적응력을 이용한 네트워크 상태에 대한 반응 확인 방법이 있다. 예를 들어 고의적으로 렉을 유발할 경우 일반 사용자는 갑자기 클릭 수가 증가한다. 반면에 봇은 그와 같은 상황을 전혀 모르고 있기 때문에 상태 변화가 없을 것이라는 점을 이용하는 것이다.

다른 방법으로는 데이터의 길이와 트래픽 도착 간격, 데이터 길이에 대한 자기 상관 함수를 사용하는 방법이다[18]. 데이터 길이의 자기 상관 함수를 이용하는 방법은 봇은 계속하여 반복된 행동을 할 것이라는 전제를 이용하고, 트래픽 도착 간격 또한 일정하고 빠르게 도착할 것이라는 가정을 바탕으로 연구가 이루어진다. 이러한 특성들을 이용하여 실시간으로 봇 탐지가 가능하며, 보조적으로 자동분류 학습을 이용해 봇 탐지의 중요특성을 파악할 수 있다.

네트워크 트래픽 기반을 이용한 방법들은 트래픽의 헤더 특성치만 연산하면 되므로 상대적으로 가볍게 동작할 수 있으며 필요한 시스템 자원도 적지만, 별도의 트래픽 도청(Traffic Tapping)이 필요하다. 봇의 동작 패턴 및 주기가 일정함과 사람의 불규칙한 패턴을 구별할 수 있다는 점을 이용하지만, 숙련도나 플레이 스타일에 따라 일반 사용자도 비슷한 패턴을 보일 수 있다. 따라서 정확도는 높지 않은 편이다. 일반적으로 실시간 대응 위주이기 때문에 탐지 규칙이 밝혀지기 쉽다는 단점을 갖는다.

2.4 HOP 기반 방법

HOP(Human Observational Proofs)란 사용자를 관찰하여 검증하는 방법으로 봇 탐지를 수행하는 것이다. 크게 사용자의 입력을 관찰하는 방법과 윈도우 이벤트 시퀀스를 분석하는 방법으로 나뉜다.

사용자의 입력을 관찰하여 검증하는 방법은 사용자의 입력을 클라이언트 측에서 수집하여 분석하는 것이다[19]. 게임을 플레이하는 봇과 사람의 입력 값들을 인공신경망(ANN; Artificial Neural Network) 등의 방법으로 분석하여 봇을 검출한다. 인공신경망의 경우 많은 시스템 자원을 소모한다는 단점이 있으나 높은 탐지율을 보여준다. 그러나 인공신경망을 이용한 탐지 방법은 은닉층의 내용이 공개되지 않기 때문에 검증이 어렵다. 또, 사용자의 입력을 관찰하여 검증하는 방법은 수집한 클라이언트의 정보를 취합한 후 해당 정보를 서버로 보내는 과정에서 봇 개발자에게 분석 당하여 수집 방법이 노출될 경우 우회될 가능성이 있다.

윈도우 이벤트 시퀀스를 분석하는 방법은 사람과 봇에서 생성된 키보드와 마우스 이벤트 시퀀스를 수집하여, 평균 시간, 표준편차와 같은 속성들을 추출하고, 그 속성을 이용하여 생성한 벡터들을 학습에 사용하였다[20]. 일반적으로 봇이 더 많은 이벤트를 생성하고 같은 종류의 이벤트 시간 간격과 연속적 이벤트 사이의 표준편차가 사람보다 더 짧다. 이는 봇은 상황 변화에 익숙하지 않거나, 상황변화에 대응하는 알고리즘이 내장되어 있지 않음을 의미한다.

HOP 기반의 탐지 방법은 데이터 자체가 봇 탐지를 위한 가공이 필요하지 않으며 신속하게 처리할 수 있기 때문에 빠른 연산이 가능하다. 그러나 필요 이상으로 키보드와 마우스 동작이 많을 경우에는 부하가 유발될 수 있다. 일반 사용자와 봇이 발생시키는 키보드·마우스 이벤트의 차이는 매우 명확하기 때문에 탐지 정확도는 높다. 그러나 클라이언트에서 키 입력, 마우스 이벤트를 기록하기 위한 별도의 모듈이 필요하고, 이것이 노출될 경우 탐지 규칙이 밝혀질 확률이 높아진다.

2.5 CAPTCHA 기반 방법

CAPTCHA(Completely Automated Public Turing Test To Tell Computers and Humans Apart) 테스트는 인간은 쉽게 풀 수 있지만 컴퓨터는 쉽게 풀지 못하는 문제를 이용하는 것이다[23]. CAPTCHA는 재전송 공격에 취약하기 때문에, 전통적인 CAPTCHA 방법으로는 봇 예방에 효율적이지 않다. 온라인 게임에 CAPTCHA를 적용하는 것에 관한 연구로는 하드웨어를 이용한 CAPTCHA[21]과 CAPTCHA를 게임 내에 구현하여 효

〔표 2〕 각 탐지 방법들의 비교

분류	적용성 (Feasibility)	분석 속도	분석 자원	정확도
사용자 행동 기반	높음	중간	낮음	매우 높음
이동경로 기반	매우 높음	중간	중간	낮음
트래픽 기반	매우 높음	높음	높음	매우 낮음
HOP 기반	중간	높음	중간	높음
CAPTCHA 기반	낮음	매우 높음	매우 높음	중간

율성을 개선하는 방법도 있다〔22〕.

CAPTCHA의 공통적인 단점은 게임에 대한 몰입도를 크게 떨어뜨린다는 것이다. 국내 다수의 MMORPG에서 CAPTCHA를 적용했으나 사용자들의 저항감이 컸던 경험이 있다. 따라서 CAPTCHA는 탐지의 주요수단으로 이용하기보다는 보조수단으로써 이용되는 것이 바람직하며, 몰입도를 해치지 않기 위해서는 CAPTCHA 질의를 발생시키는 상황을 게임 설계단계부터 반영하여 자연스럽도록 해야 효과를 거둘 수 있다. 연산에 필요한 양이 고정적이며, 작은 그림파일만 안전하게 전송하면 되기 때문에 시스템 자원 소모량은 매우 적은 반면, 게임 몰입도를 해치거나 OCR(Optical Character Recognition) 판독으로 우회가 가능하다는 단점이 있다.

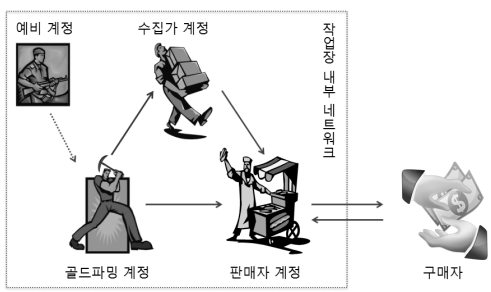
앞서 설명한 5가지의 방법은 각각 장단점을 가지고 있어 게임의 종류와 플레이 환경과 구성에 따라 적절한 방법을 선택하여야 한다. 각각의 방법의 장단점을 쉽게 알아보기 위하여 표로 구성하면 〔표 2〕와 같다.

대부분의 온라인게임회사에서 봇을 탐지하고, 봇을 이용한 사용자들을 제재하는 것으로 작업장에 대응해 왔지만, 정상적인 사용자를 봇으로 오탐(False-Positive)을 할 경우에 사용자들의 경험(User Experience)과 만족도를 크게 해칠 수 있기 때문에, 탐지범위가 넓은 방법보다는, 미탐(False-Negative)이 발생하더라도 정확도가 높은 방법들을 적용하는 것이 일반적이다. 더불어, 이러한 봇 탐지 방법들은 앞서 설명한 작업장의 3가지 유형 중 오직 골드파밍 계정만 탐지할 수 있으며, 작업장에서는 해당 골드파밍 캐릭터가 제재당할 경우, 미리 준비되어 있던 다른 계정의 예비 캐릭터로 똑같은 작업을 수행하기 때문에 제재 효과는 그리 크지 않다. 따라서 불량 사용자 그룹의 3가지 유형을 모두 탐지하고, 예비 계정까지 효과적으로 탐지할 수 있는 알고리즘이 필요하다.

III. 군집화에 기초한 불량 그룹 탐지 모델

온라인 게임 분야에서 '작업장'이라는 단어는 불량 사용자 집단이 한곳에 모여 골드파밍을 하는 장소를 지칭하는 말이지만, 불량 사용자 집단 그 자체를 뜻하기도 한다. 과거의 작업장은 자신들이 좋아하는 게임을 하면서 돈을 받기를 원하는 사람들을 고용하여 수동으로 운영하였지만, 최근 게임 봇이 발달함에 따라 상대적으로 비싼 인력 대신에 게임 봇 프로그램을 구입하여 작업장을 운영함으로써, 효율을 극대화 시키고 있다.

이러한 작업장에도 〔그림 1〕과 같이 계정간의 내부 네트워크는 존재한다. 우선 봇 프로그램을 사용하여 반복적으로 가상 재화를 습득하는 골드파밍 계정이 있다. 이러한 골드파밍 계정들이 모은 가상재화를 구매를 원하는 사람에게 쉽게 팔기 위해서 몇 개의 계정에 나누어 모아두는데 이러한 계정을 수집가 계정이라고 한다. 가상재화의 구매를 원하는 구매자가 나타났을 때 수집가 계정으로부터 가상재화를 넘겨받고, 실제 구매자에게 파는 계정이 있는데 이를 판매자 계정이라고 한다〔13〕〔14〕. 판매자 계정을 두는 이유는 많은 온라인 게임 회사들이 현금거래를 하였다고 판단이 되면 해당 계정을 제재하기 때문에, 그동안 재화를 모아둔 수집가 계정이 제재당하게 되면 그 피해가 크기 때



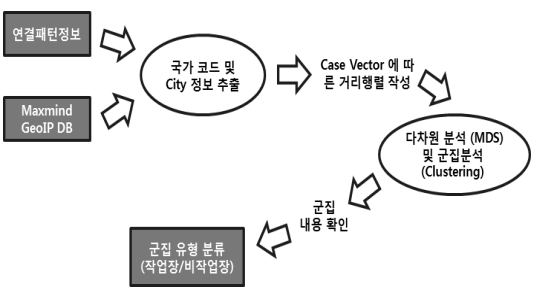
〔그림 1〕 현금거래 네트워크

문이다. 추가로 골드파밍 계정은 불법 프로그램을 이용하여 지속적으로 활동을 하기 때문에 자주 제재를 당하는데, 골드파밍 계정이 제재를 당하였을 때 그 공백을 메우기 위한 예비 계정이 존재한다[24].

기존의 연구는 골드파밍 계정을 탐지하는데 초점이 맞춰져 있다. 현재는 과거와는 달리 개별적으로 봇을 이용하는 사용자보다 작업장을 통해 조직적이고 체계적으로 불법행위가 일어나고 있기 때문에 개별적으로 봇 탐지하는 것보다는 작업장 그룹을 파악하는 것이 필요하다. 작업장 내에서의 불법 네트워크를 형성하는 집단은 물리적으로 같은 장소에 존재하는 경우가 대부분이다. 따라서 같은 집단이 이용하는 네트워크는 동일할 것이고, 이들의 연결패턴은 유사할 것이다. 연결패턴이란 클라이언트에서부터 출발한 네트워크 패킷이 서버에 들어오기까지 거치는 라우터의 IP 주소 정보를 뜻한다. 연결패턴의 라우터 IP 주소는 클라이언트의 IP 주소와 달리 클라이언트 단에서 마음대로 조작할 수 없고, 물리적으로 같은 공간에서 서로 유사하지 않은 다른 IP 주소를 가진 장치에서 접속하였다 할지라도 비슷한 시간에 같은 공간에서 출발한 패킷이 동일한 서버로 오기까지의 라우팅 경로는 유사할 가능성이 높다. 본 연구에서는 이러한 사실을 기반으로 연결패턴과 계정명의 유사성을 토대로 작업장을 탐지할 수 있는 방법을 제안한다.

제안하는 방법은 위에서 언급한 클라이언트 프로그램으로 수집된 서버로의 5 단계 (5 hop)의 추적경로를 기반으로, 추가적인 몇 가지 주요 특성들을 이용하여 각각의 거리를 구하고, 해당 특성들의 거리를 이용하여 각 로그들 간의 거리행렬을 구하고 거리행렬을 이용하여 유사한 개체들을 동일한 군집으로 묶는 군집분석을 제안한다. 제안하는 프로세스는 [그림 2]와 같다.

최초 사전에 수집한 연결패턴을 GeoIP 데이터베이스와 결합하여 각 hop 의 IP 주소로부터 국가코드 및 도시정보를 추출한다. GeoIP 데이터베이스는 IP 주소로부터 해당 IP 주소의 국가코드 및 도시정보, ISP 등의 정보를 데이터베이스화 시켜놓은 것을 말한다. 그 후 추출한 정보과 결합하여 Case Vector를 구축하고, Case Vector 내의 요소 간에 정의한 유사도에 따라 계산 후 거리행렬을 작성한다.



[그림 2] 연결패턴 정보 분석 프로세스

기존의 군집화 알고리즘에서 사용하는 특성치 별 동일한 거리 측정 방법을 적용하기 때문에 본 연구의 특성치에 적용하는 것은 바람직하지 않다. 제안하는 방법론에서 사용하는 특성치는 명목변수이기는 하나 속성값 간의 거리를 같고 다름으로만 표현하는 것으로는 유사한 집단을 동일 집단으로 군집화하기 어렵기 때문이다. 연결패턴 정보 및 계정명 특성치는 값의 일부분만이 유사하여도 동일 집단일 가능성이 있기 때문에, 본 연구에서는 계정간의 유사도를 구하기 위해 각 특성치에 적합한 거리 계산 방법을 제안한다. 제안하는 특성치 별 거리 계산 방법은 기존의 모든 변수에 동일한 거리를 측정 방법을 적용하는 것보다 작업장 탐지에 효율적일 것으로 기대된다.

특성치별 특화된 거리행렬을 기반으로 군집분석을 수행하고, 군집 결과를 분석하여 작업장 그룹을 파악한다. 군집분석이란 관측대상들 간에 어떤 공통 특징을 찾아 비슷한 특징을 갖는 관측치들을 군집으로 형성하는 방법이다. 즉, 분석하고자 하는 변수를 서로 유사한 특징을 지닌 대상들을 하나의 집단으로 묶는 기법이다. 이를 통해 집단내부에 존재하는 분석 대상들을 서로 동질적인 군집을 만들 수 있고, 집단 간은 당연히 서로 이질적이게 된다. 작업장으로 탐지된 그룹을 실제 제제 계정과 비교하여 제안한 방법에 따른 군집화 결과를 검증한다. 추가적으로 군집화의 시각화를 위해 다차원분석을 통해 다차원 특성치를 이차원으로 줄여, 2차원 평면에 시각화하는 작업을 수행한다. 이러한 시각화 기법은 군집화 결과를 직관적으로 평가할 수 있게 하여, 실제 현업에 적용할 때 큰 이점을 제공한다.

본 논문에서 제안하는 불량그룹 탐지에 대한 특성치로 컴퓨터 고유 주소(MAC), 계정명(Account), 경로별 IP 주소(IP1~5), 이에 따른 국가코드(CRcode1~5) 및 도시정보(CTname1~5)를 활용한다.

MAC은 사용자 컴퓨터의 고유 주소이다. MAC 주소가 동일하다는 것은 동일한 장치에서 접속을 시도한 것으로 볼 수 있으므로 특성치로 활용하였다. Account는 각 사용자 계정명으로, 작업장에서 타인

의 명의로 자신들이 직접 계정을 생성할 때 관리의 편의를 위해서 시리즈 계정을 대량으로 생성하는 경우가 많기 때문에 이를 주요 특성치로 선정하였다. 시리즈 계정이란 동일한 문구에 뒤의 숫자만 바꾸면서 생성되어 게정명의 일부가 유사한 계정을 말한다. 예를 들면 s15e022, s15e023, s15e025 등을 시리즈 계정이라고 할 수 있다. IP1~5는 클라이언트로부터 서버까지 라우팅 경로 상에 있는 5 hop 의 IP 주소이다. CRcode는 해당 IP 주소로부터 추출한 국가코드 2자리를 말하며 이 국가코드는 RFC 1631문서를 따른다[25]. CTname 또한 마찬가지로 해당 IP 주소로부터 추출한 도시이름을 말한다.

각 특성치에 적합한 유사도 측정 방법은 다음과 같다. 사용자간의 거리는 두 개체가 어느 정도 유사한지 판단하는 수치로 완전히 동일하다면 0, 완전히 다르다면 1이라고 정의하고, 각 개체간의 거리(유사도)는 0과 1사이의 수치로 나타낸다.

- MAC : MAC 주소가 비슷하다고 해서 실제 거리와 비슷하다는 사실은 보장이 되지 않으므로 거리는 '같다'와 '다르다'만 검사한다. MAC값이 서로 같으면 0, 다르면 1로 설정한다. 이를 통해 동일한 PC 에서 접속이 이루어졌는지를 확인할 수 있으며, 동일한 PC 에서 접속한 경우 Case Vector 간 거리가 가깝게 나오게 된다.
- Account : 알고리즘은 Levenshtein Distance를 사용한다. Levenshtein Distance는 Edit Distance라고도 하며, 두 문자열의 비슷한 정도를 측정하기 위해 고안된 알고리즘으로 원본문자열을 대상문자열로 변형시키기 위해 삭제, 추가, 수정이 필요한 횟수를 구하는 알고리즘이다[26]. 이를 통해 동일 작업장에서 접속한 시리즈계정인지를 추정하여, 동일한 작업장에서 생성하고 관리하는 것으로 보이는 시리즈계정에서의 접속일 경우, 두 case vector 간 거리가 가깝게 된다. 이 과정을 거쳐 얻은 정수를 두 문자열 중 긴 문자열의 길이로 나누게 되면 0과 1의 사이의 거리가 나오게 된다. 예를 들어 'partner'와 'parents'의 Levenshtein Distance를 구하면, 두 단어는 3번의 수정 연산이 필요하다. (partner ; t->e, e->t, r->s ; parents) 두 단어는 길이가 똑같이 7이기 때문에 Levenshtein Distance(partner, parents) = 3/7 ≒ 0.4286이 된다.
- IP 1~5 : IP 주소는 '.' 으로 분리된 네 개의 바이트로 구성되어 있는데, 각 바이트가 위치한 각 위치의 값이 순차적으로 A, B, C, D클래스가 되고, 각 클래스는 위치 정보를 가진다. A에서부터 D로 갈수록 IP 주소의 위치정보가 세분화되기 때문에, 두 개의 IP 주소를 비교하기 위해서는 클래스별 순차적 비교가 필요하다. 두 IP 주소가 완전히 같으면 0, C클래스까지 같다면, 0.25, B클래스까지만 같다면 0.5, A클래스까지만 같다면 0.75, 완전히 다르면 1로 설정하여 더한 뒤 5로 나눠준다. 이를 통해 동일한 라우팅 경로를 통해 접속을 했는지를 판정할 수 있으며, 동일한 라우팅 경로를 통한 접속일 경우 두 case vector 간 거리가 가깝게 된다. 추가적으로, IP 1~5까지의 패턴을 앞과 뒤를 하나씩 줄여가며 비교하여 거리가 최소가 되는 지점을 찾는다. 예를 들어 A, B의 패턴이

$$\begin{aligned} A &= 192.168.0.1 - 163.152.127.1 \\ &- 172.0.0.1 - 10.0.0.1 - 201.172.6.8 \\ B &= 192.168.10.1 - 192.168.0.1 \\ &- 163.152.127.1 - 172.0.0.1 - 10.0.0.1 \end{aligned} \quad (1)$$

라고 하였을 때, IP 주소 5개를 모두 비교하였을 때 A와 B의 IP 주소의 거리는

$$d_{ip} = \frac{(0.5+1+1+1+1)}{5} = 0.9 \quad (2)$$

이 되지만 길이를 4로 줄인 뒤에는

$$\begin{aligned} A_{b1} &= 192.168.0.1 - 163.152.127.1 \\ &- 172.0.0.1 - 10.0.0.1 \\ B_{f1} &= 192.168.0.1 - 163.152.127.1 \\ &- 172.0.0.1 - 10.0.0.1 \end{aligned} \quad (3)$$

이 되어 A_{b1}와 B_{f1}의 IP 주소패턴이 동일해진다. 하지만 IP 주소가 1개 비어있으므로, 그 자리에 1을 채워 IP 주소패턴이 5개 모두 동일할 때와 형평성을 기한다. 위의 예제에서 A_{b1}과 B_{f1} 의 거리는

$$d_{ip} = \frac{0+0+0+0+1}{5} = 0.2 \quad (5)$$

가 되고, 이 값은 A와 B가 가질 수 있는 최소의 거리가 된다.

- CRcode 1~5, CTname 1~5 : CRcode와 CTname 역시 1~5까지를 패턴 하나로 묶어

거리를 계산한다. IP 주소와 유사하게 각 개체의 CRcode1~5를 앞과 뒤를 하나씩 줄여가며 비교한다. 그 후 두 개체가 완전히 같게 되는 최대 길이 MAX(Len)을 구하고, 이를 5로 나눈 값이 유사도가 된다. 거리는 1-유사도로 정의한다. 이를 통해 비록 IP 주소는 다르다 할지라도, 경유하여 접속한 국가 및 도시가 같다면 두 case vector 간 거리가 가깝게 되도록 한다. 예를 들어

A=RU-JP-US-PT-US,

B=RU-JP-CN-US-US

라고 하면 두 개체가 완전히 같게 되는 최대 패턴은 A의 앞에서 2개의 패턴 RU-JP 와 B의 앞에서 2번째의 패턴 RU-JP 이으므로 MAX(len) = 2를 갖게 된다. 같은 예로 KR-KR-KR-KR-KR, @P-KR-KR-KR-KR 은 MAX(len)=4가 된다.

두 계정간의 거리는 위의 각 특성치로 구성된 두 case vector 간 유클리드 거리로 산출한다. 예를 들어 모든 특성치를 선택하였을 때 각 계정간의 거리를 식으로 표현하면 다음과 같다.

$$D_{i,j} = \sqrt{\begin{matrix} d(Account_i, Account_j)^2 + \\ d(MAC_i, MAC_j)^2 + d(IP)^2 + \\ d(CRcode)^2 + d(CTname)^2 \end{matrix}} \quad (6)$$

거리행렬을 작성 후 K-means 알고리즘으로 case vector 들에 대해 군집분석을 실시하여, 접속패턴이 유사한 case 들이 같은 군집에 속하도록 한다. K-means 알고리즘을 사용하는데 필요한 초기 값 K는 Root Mean Square Standard Deviation(이하 RMS SD) 값과 그 다음의 Maximum Distance from Seed to observation(이하 MDS) 값을 비교를 하여 결정한다. RMS SD 값은 군집 내 개체들 간의 거리 평균 제곱근이며, 그 다음의 MDS는 군집 내 개체 중 seed와 거리가 가장 먼 개체와의 seed 간 거리로, 두 값 모두 작을수록 군집화가 잘 된 것이다. 또 각 군집에 속해있는 개체 수도 참고하였다.

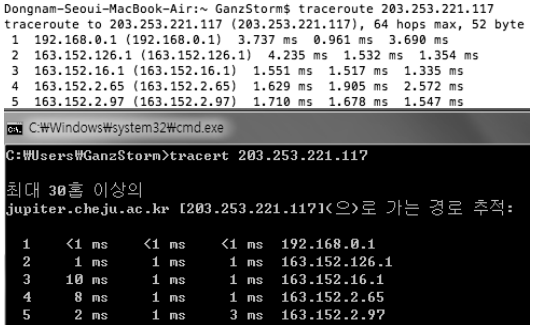
제안하는 각 특성치의 조합 중 영향력이 높은 특성치를 선별하기 위하여, 아래와 같은 3종류의 실험군을 사용하였다.

1. Case Vector = { IP1, IP2, IP3, IP4, IP5, CRcode1, CRcode2, CRcode3, CRcode4, CRcode5, CTname1, CTname2, CTname3, CTname4, CTname5, Account, MAC }
2. Case Vector = { IP1, IP2, IP3, IP4, IP5, CRcode1, CRcode2, CRcode3, CRcode4, CRcode5, CTname1, CTname2, CTname3, CTname4, CTname5, MAC}
3. Case Vector = { IP1, IP2, IP3, IP4, IP5, CRcode1, CRcode2, CRcode3, CRcode4, CRcode5, CTname1, CTname2, CTname3, CTname4, CTname5, }

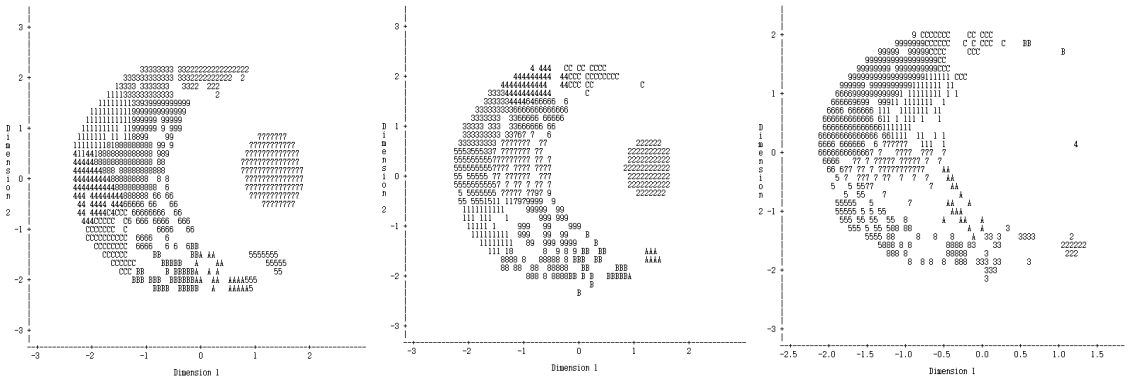
첫 번째 실험군은 제안하는 특성치를 모두 활용하였으며, 두 번째 실험군은 시리즈 계정명을 통해 작업장에서 사용하는 계정들을 탐지하는 Account에 대한 Levenshtein distance를 제외하였다. 세 번째 실험군은 Levenshtein distance와 각 컴퓨터의 고유주소인 MAC 주소에 대한 distance를 제외하여 순수 라우팅 정보(5 hops 정보, 국가코드, 도시이름)만 활용하였다.

IV. 실험 및 결과 분석

본 논문에서 제안하는 군집화 기반 작업장 탐지 모델을 국내 최대의 MMORPG 회사에 적용하여 그 효용성을 평가하였다. 연결패턴 정보를 얻기 위해서, 게임 클라이언트로부터 서버로의 5 단계 (5 hop)의 추적경로(traceroute) 정보를 수집하였다. 〔그림 3〕은 연결패턴 정보의 예시로, 서로 다른 PC라 하더라도 정적라우팅을 이용하는 환경이면서, 같은 네트워크 대역에 위치하고 있다면, 지리적으로 같은 장소에서 같



〔그림 3〕 연결패턴 정보의 유효성



〔그림 4〕 다차원 분석 뒤의 군집 분포 (왼쪽부터 1번, 2번, 3번 실험군)

은 회선을 이용하여 동일한 곳으로 전송되는 패킷의 라우팅 경로는 일치하게 된다. 마찬가지로, 서로 다른 두 대 이상의 PC 들이 같은 네트워크 대역에 위치하고 있지 않더라도, 지리적으로 유사한 장소에 위치하며 동일한 시간대에 접속을 한다면 지역적으로 동일한 ISP를 이용할 확률도 높게 되고 동적라우팅을 이용하여 전송된다 하더라도 비슷한 라우팅 경로를 통해 전송될 가능성이 매우 높다. 따라서 작업장과 같이 대량의 컴퓨터들이 같은 시간대에 지리적으로 인접해 있는 네트워크에서 대규모의 접속을 동일한 목적지로 하는 경우, 타 트래픽과 명확히 다른 패턴을 보이는 접속군이 형성되므로 이를 통해 작업장의 접속을 분류해 낼 수 있게 된다.

본 실험에서는 샘플링된 게임서버에 수집된 클라이언트 접속 로그를 사용하였다. 이 로그는 로그인 시간, 계정명, IP 주소, MAC 주소를 포함하고 있다. IP 주소의 국가 및 도시 정보를 추출하기 위해 www.maxmind.com의 GeoIP 데이터베이스를 사용하였다. 본 실험에서는 2010년 5월 15일부터 6월 13일까지의 로그 31,292,433건 중 5000건을 랜덤 추출하여 사용하였다. 본 연구에서는 군집 분석을 위해 군집의 수 K를 사전에 정의하여 상호배반적인 K개의 군집을 형성하는 K-means 알고리즘을 사용하였다. 해당 알고리즘은 계산시간이 오래 걸리지 않으므로 대용량 자료의 경우 유용하게 쓰이며, 사용자가 군집 수(K)를 정할 수 있어 학습 과정에 개입할 수 있기 때문이다. 군집분석은 다양한 형태의 데이터에 적용이 가능하고, 분석방법의 적용이 용이하다는 장점이 있지만, 가중치와 거리를 결정하는 것이 어렵고, 초기 군집 수 K가 데이터 구조에 적합하지 않으면 좋은 결과를 얻을 수 없고, 사전에 주어진 목적이 없으므로 결과를 해석하는 데 있어서 어렵다는 단점이 있다.

〔표 3〕 각 실험군의 유사 경로 비율 비교

Cluster	1번 실험군			2번 실험군			3번 실험군		
	최대 유사 경로 수	총 관측치 수	유사 경로 비율(%)	최대 유사 경로 수	총 관측치 수	유사 경로 비율(%)	최대 유사 경로 수	총 관측치 수	유사 경로 비율(%)
1	38	378	10	8	288	2.78	38	221	17.19
2	280	290	96.6	1838	1838	100.00	66	100	66.00
3	47	189	24.9	2	352	0.57	274	338	81.07
4	51	363	14	42	289	14.53	1838	1838	100.00
5	16	35	45.7	97	337	28.78	97	347	27.95
6	56	347	16.1	12	146	8.22	19	377	5.04
7	1838	1838	100	26	230	11.30	115	277	41.52
8	71	274	25.9	55	397	13.85	55	467	11.78
9	115	300	38.3	155	281	55.16	2	399	0.50
A	306	433	70.7	66	91	72.53	13	98	13.27
B	64	248	25.9	264	362	72.93	1	6	16.67
C	97	305	31.8	321	389	82.52	321	532	60.34
평균			41.66			38.60			36.78

〔표 4〕 7번 군집의 로그 중 일부

Account	IP1	IP2	IP3	IP4	IP5	CR1	CR2	CR3	CR4	CR5	CT1	CT2	CT3	CT4	CT5
**ggtt88	175.12.***.254	10.6.***.1	61.251.***129	61.251.***.13	211.108.***.9	CN	@P	KR	KR	KR	changsha	@P	seoul	seoul	seoul
**angkss	175.12.***.254	10.6.***.1	61.251.***129	61.251.***.13	211.108.***.9	CN	@P	KR	KR	KR	changsha	@P	seoul	seoul	seoul
**sry990	175.12.***.254	10.6.***.1	61.251.***129	61.251.***.13	211.108.***.9	CN	@P	KR	KR	KR	changsha	@P	seoul	seoul	seoul
**tjdwls	175.12.***.254	10.6.***.1	61.251.***129	61.251.***.13	211.108.***.9	CN	@P	KR	KR	KR	changsha	@P	seoul	seoul	seoul
**j1987	175.12.***.254	10.6.***.1	61.251.***129	61.251.***.13	211.108.***.9	CN	@P	KR	KR	KR	changsha	@P	seoul	seoul	seoul
**vud70	175.12.***.254	10.6.***.1	61.251.***129	61.251.***.13	211.108.***.9	CN	@P	KR	KR	KR	changsha	@P	seoul	seoul	seoul
**vixzio	175.12.***.254	10.6.***.1	61.251.***129	61.251.***.13	211.108.***.9	CN	@P	KR	KR	KR	changsha	@P	seoul	seoul	seoul

본 실험에서는 군집화의 목적에 부합하고 해당 데이터의 크기에 적합한 군집수를 정하기 위해 반복적인 실험을 거쳐 동일 그룹이 세분화되지 않은 수준의 값을 선택하였다. 해당 데이터에 대한 군집화에서는 12개의 군집이 적절한 것으로 나타났다.

〔그림 4〕는 세 가지 실험군을 다차원 분석(MDS; Multidimensional Scaling) 뒤 군집분석 후 그 분포를 나타낸 결과이다. 세 실험군 모두 다소 비슷한 모양을 가지고 있다. 거리행렬이 다차원이기 때문에 다차원 분석을 통하여 2차원으로 축소시킨 뒤 시각화하였다. 〔그림 4〕의 1번 실험군에서 보는바와 같이 다른 군집과는 다르게 7번 군집(2번 실험군의 경우 2번 군집, 3번 실험군의 경우 4번 군집)의 경우 다른 군집들과 떨어져서 밀집하여 있다. 이러한 시각화를 통해 군집화의 성능을 직관적으로 파악할 수 있고, 군집간의 거리를 쉽게 파악할 수 있다.

〔표 3〕은 세 가지 실험군의 각 군집에 대한 최대 유사 경로 비율 비교표이다. 유사 경로 비율이란, 해당 군집의 데이터들 중 같거나 80% 이상 유사한 즉 IP1~IP5의 distance가 0.2 이하인 데이터들의 비율을 의미한다. 제안한 특성치 모두를 사용한 1번 실험군이 평균 유사 경로 비율(최대 유사경로 수 / 총 관측치 수)이 가장 높음을 알 수 있다. 이는 1번 실험군이 2, 3번 실험군에 비해 연결패턴이 비슷한 관측치들 간에 군집이 잘 형성되어 있음을 보여준다.

1번 실험군의 군집 내 유사한 경로의 비율을 살펴보면, 그 값이 높게 나타나는 2번, 7번, A번 군집이 작업장으로 의심 되었다. 7번 군집은 〔표 4〕에 나온 패턴과 동일한 로그들로만 이루어져 있어 유사 경로 비율이 100%로 나타났다. 또한 7번 군집의 IP1 의 경우 국가코드가 중국을 뜻하는 CN 으로, 중국에 위치한 이용자들이 VPN 기술을 통한 우회접속을 하였다는 것을 제안된 기술을 이용하여 용이하게 탐지할 수 있었다. 추가적으로 군집들의 내용을 살펴본 결과 2번과 A번 군집이 작업장으로 의심되나, 7번 군집과는 다르게 2번과 A번 군집은 일부 노이즈를 가지고 있다.

제안한 방법의 성능을 평가하기 위해 EM(Expectation Maximization) 군집분석을 추가적으로 수행하여 제안한 방법과 비교하였다. EM 알고리즘은

〔표 5〕 제안한 방법과 EM 군집분석의 비교표

Cluster	Our Method				EM Clustering			
	최대 유사 경로 수	총 관측치 수	유사 경로 비율	군집 내 평균 거리	최대 유사 경로 수	총 관측치 수	유사 경로 비율	군집 내 평균 거리
1	38	378	10	2.26	1	288	0.3	2.35
2	280	290	96.6	0.83	274	313	87.5	1.04
3	47	189	24.9	1.97	2	319	0.6	1.97
4	51	363	14	2.24	17	116	14.7	2.31
5	16	35	45.7	1.26	1	90	1.1	1.67
6	56	347	16.1	2.23	35	194	18	2.23
7	1838	1838	100	0.7	1838	1890	97.2	0.9
8	71	274	25.9	1.78	99	182	54.4	1.73
9	115	300	38.3	2.06	118	666	17.7	2.11
A	306	433	70.7	1.01	321	567	56.7	1.57
B	64	248	25.9	1.83	66	178	37	1.81
C	97	305	31.8	2	115	197	58.4	2.1
평균			41.66	1.68			36.97	1.82

〔표 6〕 2010년 상반기 / 2011년 7월 22일 기준, 각각의 제재 계정 목록과의 비교표

	2010년 상반기 기준			2011년 7월 22일 기준			비고	
Cluster	제재 계정 수	전체 계정 수	비율	제재 계정 수	전체 계정 수	비율	상승	비율상승
2	37	248	14.9194	109	248	43.9516	72	29.0323
7	103	687	14.9927	349	687	50.8006	246	35.8079
A	84	167	50.2994	119	167	71.2575	35	20.9581

K-means 알고리즘과 흡사하지만 K-means 알고리즘은 유클리드 거리를 사용하는 것에 비해 EM 알고리즘은 log-likelihood 함수를 사용하여 모델의 적합성을 평가하는 확률기반의 알고리즘이다. 각 방법에 따른 유사경로 비율과 군집 내 평균거리는 〔표 5〕와 같다. K-means를 활용하는 방법이 EM 군집분석에 비해 유사한 데이터끼리 군집을 형성했음을 의미하는 군집 내 평균거리가 낮고, 유사 경로 비율이 높아 군집이 비교적 잘 형성되었다고 할 수 있다.

제안한 방법의 탐지율을 유추하기 위해, 회사 측으로부터 2010년 상반기까지의 제재 계정 목록을 받아 작업장이라고 의심되는 2번, 7번, A번 군집의 계정들과 비교하여 보았다. 〔표 6〕을 보면, 탐지율이 매우 낮은 것을 볼 수 있는데, 이는 우리의 방법은 작업장의 3가지 유형의 모든 계정과 예비 계정까지 모두 찾아내는 것에 반해, 현재까지 온라인게임회사들에서는 봇 탐지결과에 의존하여 제재를 하고 있었기 때문에, 작업장의 3가지 유형의 계정 중 골드파밍 계정, 1가지 유형의 계정만 제재했기 때문이다. 또한, IP 주소는 제재 시점에 따라 실제 이용자와 탐지 시점의 IP 주소 이용자가 달라질 수 있어서, 온라인게임회사들은 본 논문에서 제시된 결과와 같이 추가적인 기술적 근거가 제시되지 않는 한 현재까지는 작업장이라고 의심되는 IP 주소를 제재의 근거로 활용하지 못해왔던 것도 이유 중의 하나이다.

이를 입증하기 위해 2011년 7월 22일까지의 제재 계정 목록을 추가로 받아 비교하여 본 결과 제재 계정 수와 비율이 큰 폭으로 상승하였고, 전체 12개의 군집 중에서 비율이 20% 이상 상승한 군집은 2번, 7번, A번 밖에 없었다.

〔표 7〕 각 탐지 방법들의 장단점 비교표

분 류	장 점	단 점
사용자 행동 기반	- 높은 정확도 및 탐지율 - 탐지 규칙이 잘 노출되지 않도록 조절가능	- 데이터 처리 연산량, 예외처리 등의 문제 - 어떤 행동을 통해 구별할 것인가의 문제 - 사용자들의 평균적인 행동에 대한 깊은 이해가 필요 - gold farming 형태의 계정만을 탐지
이동경로 기반	- 게임 플레이에 영향을 미치지 않음	- 대규모 맵에서의 연산 문제 - 이동 시 랜덤성이 추가된 신형 봇에 대한 탐지 문제 - 숙련된 사용자에 대한 오탐 문제 - gold farming 형태의 계정만을 탐지
트래픽 기반	- 요구 시스템자원이 낮음	- 별도의 트래픽 도청이 필요 - 숙련도나 플레이스타일에 따른 오탐 문제 - 탐지 규칙이 밝혀지기 쉬움 - 정확도가 높지 않음 - gold farming 계정만을 탐지
HOP 기반	- 데이터 가공이 필요치 않음 - 빠른 연산 가능 - 높은 정확도	- 키보드와 마우스 동작이 많을 시 부하 유발 - 이벤트 기록을 위한 별도의 모듈 필요 - 탐지 규칙이 밝혀지기 쉬움 - gold farming 계정만을 탐지
CAPTCHA 기반	- 요구 시스템 자원이 매우 낮음 - 분석속도가 가장 빠름	- 쉽게 우회 가능 - 사용자들의 게임 몰입도 저해 - gold farming 계정만을 탐지
제안하는 방법	- 작업장 전체 네트워크 탐지 가능 - IP변조 및 우회에 면역 - 예비 불량사용자 탐지 가능	- 데이터 가공 필요 - 연결패턴을 기록할 별도 모듈 필요 - 작업장 주변에서 접속하는 일반사용자들의 오탐 문제

따라서 제안하는 방법으로 탐지되는 계정들은 이후에 불량사용자로 판정이 날 가능성이 높기 때문에, 이들을 집중적으로 모니터링 하여 효과적으로 관리할 수 있다. 또한, 이 목록 중에는 기존의 탐지방법으로 나타나지 않는 수집가 계정 및 판매원 계정도 있기 때문에, 추가적으로 다른 방법과 결합하여 작업장임이 확실해졌을 때 작업장에 속해있는 계정들을 한 번에 제재를 가한다면, 작업장에 큰 피해를 줄 수 있다.

기존의 불량사용자 탐지에 관한 연구들과 제안하는 방법의 장단점을 비교해보면 〔표 7〕과 같다.

V. 결 론

기존에 온라인게임 보안과 관련된 연구들은 작업장(gold farmer)에 대한 분류기법 자체 보다는 불량사용자들이 주로 게임 봇을 사용한다는 사실에 기인하여 게임 봇을 사용한 이용자를 탐지하는 것에 초점이 맞추어져 왔었다. 이러한 기존의 방식은 작업장 네트워크 전체를 탐지하지 못하고, 작업장 네트워크의 구성원들 중 gold farming을 하는 구성원만을 탐지하게 되는 단점이 존재한다. 또한 게임서비스회사 역시 봇 탐지 알고리즘들에 의해 탐지된 계정과 관련된 IP 주소에 대해서만 제재 또는 접속을 차단하는 방식을 취해왔다. 하지만 이런 탐지 및 제재 방법들은 제재된 계정을 보완하는 예비 계정 도입과 IP 주소 변조 및 VPN 기술로 무력화 되며, 봇 탐지에 초점을 맞춘 방법은 작업장의 일부만을 탐지할 수 있다는 한계점을 가진다. 이러한 문제점을 해결하기 위해 본 연구는 연결패턴 정보를 이용하여 유사 그룹을 탐지함으로써 작업장 전체를 탐지할 수 있는 군집화 기반의 탐지 모델을 제안하였다.

본 연구에서 제안하는 모델은 컴퓨터 고유 주소(MAC 주소), 라우터 상의 상위 5개까지의 IP 주소와 이에 따른 국가 및 도시 정보를 활용하였고, 추가적으로 계정명을 특성치로 고려하였다. 단순히 라우팅 정보만을 활용할 경우에는 작업장 근처의 일반사용자들이 작업장과 같은 ISP 를 이용하여 비슷한 시간대에 접속할 경우 오탐이 발생할 수 있지만, 본 모델에서는 작업장은 계정의 이름을 시리즈화 된 유사 계정을 사용한다는 점과, IP 주소는 수시로 변경할 수 있더라도, 불량행위에 이용되는 PC 의 하드웨어 정보는 접속 시 수시로 변경하기 어려운 점을 고려하여 이 추가적인 특성치를 고려하여 정확도를 높일 수 있었다. 군집화의 효율을 높이기 위해 각 특성치에 적합한 거리 산출 방법을 제안하고, 이를 국내 최대의 MMORPG 회사의 실제 로그에 적용하여 그 효용을 입증하였다. 제안하는 모델은 각 연결정보의 특성치별 적합한 거리 산출 방법을 적용하여 기존의 군집화 방법에 비해 작업장 탐지의 성능에 높은 성능을 나타내었다. 제안한 방법에 의해 탐지된 그룹들은 시간이 지나면서 다른 그룹에 비해 불량사용자 비율이 급격히 증가하는 것을 보이는데, 이를 통해 제안하는 방법이 효과적으로 불량사용자들을 군집화 하였다고 할 수 있다.

제안하는 모델은 기존의 봇 탐지 알고리즘에서는 탐지할 수 없는 수집가 계정 및 판매자 계정도 함께 탐지할 수 있다. 이에 작업장 탐지 및 제재를 시행할 때 작업장이 수집해둔 가상 재화를 현금화하기 전에 수집가 계정을 포함하여 제재를 가한다면 해당 작업장의 활동을 억제하는데 큰 효과를 보일 것으로 기대된다.

참고문헌

〔1〕 Davis, R., "Welcome to the new gold mines," The Guardian., http://www.guardian.co.uk/technology/2009/mar/05/virtual-world-china, Mar. 2009.

〔2〕 Castronova, E., "Virtual goods at GDC," TerraNova., http://terranova.blogs.com/terra_nova/2010/03/virtual-goods-at-gdc.html, Mar. 2010.

〔3〕 최화재, 우지영, 김휘강, "온라인게임 계정도용 탐지모델에 관한 연구," 한국게임학회 논문지, 11(6), pp.81-94, Dec. 2011.

〔4〕 M. van Kesteren, J. Langevoort and F. Grootjen, "A step in the right direction; botdetection in mmorpgs using movement analysis," In Proceedings of the 21th Belgian-Dutch Conference on Artificial Intelligence (BNAIC2009), Oct. 2009.

〔5〕 A.R. Kang, J.Y. Woo, J.Y. Park and H.K. Kim, "Online game bot detection based on party-play log analysis," Adv Comp Sci App in press, 2011.

〔6〕 R. Thawonmas, Y. Kashifuji and K.T. Chen, "Detection of mmorpg bots based on behavior analysis," Proceedings of the 2008 International Conference on Adv-

ances in Computer Entertainment Technology, pp. 91-94, Dec. 2008.

〔7〕 M.A. Ahmad, B. Keegan, J. Srivastava, D. Williams, and N. Contractor, "Mining for gold farmers: automatic detection of deviant players in mmogs," Computational Science and Engineering, IEEE, vol. 4, pp. 340-345, Aug. 2009.

〔8〕 K.T. Chen and L.W. Hong, "User identification based on game-play activity patterns," Digital Signal Processing, ACM, pp. 7-12, Jan. 2007.

〔9〕 S. Yeung, J.C.S. Lui, J. Liu, and J. Yan, "Detecting cheaters for multiplayer games: theory, design and implementation," Networking Issues in Multimedia Entertainment, Citeseer, pp. 1178-1182, Jan. 2006.

〔10〕 M. Varvello and G.M. Voelker, "Second life: a social network of humans and bots," Network and Operating Systems Support for Digital Audio and Video, ACM, pp. 9-14, June 2010.

〔11〕 A.R. Kang, J.Y. Woo, and H.K. Kim, "Data and text mining of communication patterns for game bot detection," Proceedings of the 3th International Conference on Internet 2011, pp. 495-500, Dec. 2011.

〔12〕 H.M Kwon and H.K. Kim, "Self-similarity based bot detection system in mmorpg", Proceedings of the 3th International Conference on Internet 2011, pp. 477-481, Dec. 2011.

〔13〕 K.M. Woo, H.M Kwon, H.C Kim, C.K. Kim and H.K Kim, "What can free money tell us on the virtual black market," ACM SIGCOMM, vol. 41, no. 5, pp. 392-393, Oct. 2011.

〔14〕 H. Itsuki, A. Takeuchi, A. Fujita and H. Matsubara, "Exploiting mmorpg log data toward efficient rmt player detection", Proceeding ACE '10 Proceedings of the 7th International Conference on Advances in Computer Entertainment Technology, Nov. 2010.

〔15〕 S. Mitterhofer, C. Platzer, C. Kruegel and E. Kirda, "Server-side bot detection in massively multiplayer online games," IEEE Security & Privacy, vol. 7, no. 3, pp. 29-36, May 2009.

〔16〕 R. Thawonmas, M. Kurashige, and K.T. Chen, "Detection of landmarks for clustering of online-game players," International Journal of Virtual Reality, vol. 6, no. 3, pp. 11-16, 2007.

〔17〕 K.T. Chen, J.W. Jiang, P. Huang, H.H. Chu, C.L. Lei, and W.C. Chen, "Identifying mmorpg bots: A traffic analysis approach," EURASIP Journal on Advances in Signal Processing, vol. 2009, Jan. 2009.

〔18〕 S. Hilaire, H. Kim, and C. Kim, "How to deal with bot scum in mmorpgs?," Communications Quality and Reliability, pp. 1-6, June 2010.

〔19〕 S. Gianvecchio, Z. Wu, M. Xie, and H. Wang, "Battle of botcraft: fighting bots in online games with human observational proofs," Computer and Communications Security, pp. 256-268, Nov. 2009.

〔20〕 H. Kim, S. Hong, and J. Kim, "Detection of auto programs for mmorpgs," Computer Science, vol. 3809, pp. 1281-1284, 2005.

〔21〕 P. Golle and N. Ducheneaut, "Preventing bots from playing online games," Computers in Entertainment, vol. 3, no. 3, pp. 3-3, July 2005.

〔22〕 R.V. Yampolskiy and V. Govindaraju, "Embedded noninteractive continuous bot detection," Computers in Entertainment, vol. 5, no. 4, pp. 1-11, Mar. 2008.

〔23〕 L. von Ahn, M. Blum, N.J. Hopper and J. Langford, "CAPTCHA: Using hard ai problems for security," Proceeding EUROCRYPT'03 Proceedings of the 22nd international conference on Theory and

applications of cryptographic techniques, pp. 294-311, 2003.
〔24〕 이동원, "작업장하면서 원형탈모증에 걸렸어요. 작업장주를 만나다," 게임웹진 인벤, http://www.inven.co.kr/webzine/news/?news=37769, Aug. 2011.
〔25〕 http://www.faqs.org/rfcs/rfc1631.html
〔26〕 http://en.wikipedia.org/wiki/Edit_distance

〈著者紹介〉

서 동 남 (Dongnam Seo) 학생회원
2009년 8월: 제주대학교 전산통계학과 학사
2012년 2월: 고려대학교 정보보호대학원 석사수료
〈관심분야〉 온라인게임 보안, 네트워크 보안, 데이터마이닝, 소셜 네트워크

우 지 영 (Jiyoung Woo) 정회원
2000년: KAIST 산업공학과 학사
2002년: KAIST 산업공학과 석사
2006년: KAIST 산업공학과 박사
2006년: 삼성화재 고객관계관리 부서
2008년: 미국 아리조나대학 인공지능연구실
2011년: 고려대학교 정보보호대학원 연구교수
〈관심분야〉 온라인게임 보안, 데이터마이닝

우 경 문 (Kyung-moon Woo) 정회원
1995년: 공군사관학교 전산과 (학사).
2007년: 서울대학교 전기, 컴퓨터공학부(석사)
2012년: 서울대학교 전기, 컴퓨터공학부(박사)
〈관심분야〉 무선랜, 이동통신, 네트워크 보안

김 종 권 (Chong-kwon Kim) 정회원
1982년: 미국 조지아 공과대학교 산업공학과 석사
1987년: 미국 일리노이 대학교 전산학과 박사
1984년~1987년: IBM 산호세 연구소 연구조원
1987년 1월~1991년: 미국 Belcore 통신연구소 연구원
1991년~현재: 서울대학교 전기·컴퓨터공학부 교수
〈관심분야〉 차세대인터넷, 초고속라우터, 이동통신

김 휘 강 (Huy Kang Kim) 종신회원
1998년 2월: KAIST 산업경영학과 학사
2000년 2월: KAIST 산업공학과 석사
2009년 2월: KAIST 산업 및 시스템 공학과 박사
2004년 5월~2010년 2월: 엔씨소프트 정보보안실장, Technical Director
2010년 3월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 온라인게임 보안, 네트워크 보안, 네트워크 포렌직, 침입탐지시스템, 봇넷탐지