온라인 게임 환경에서 게임 봇 탐지 기법 사례조사 연구

윤태복*
*서일대학 컴퓨터소프트웨어과
tbyoon@seoil.ac.kr

A Case Study on the Game Bots Detection Method in Online Game Environment

Taebok Yoon*
*Dept of Computer Software, Seoil University

요 약

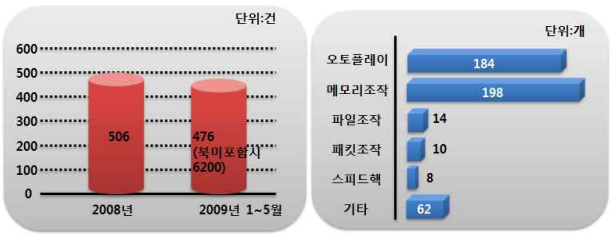
IT기술의 발달과 함께 온라인 게임 시장은 시장 규모가 늘어나고 고부가가치 산업으로 인식되고 있다. 하지만, 악의적인 프로그램을 이용한 게임 운용은 정상적인 게임을 즐기는 사용자에게 큰 피해를 주고 있다. 본 논문은 온라인 게임 환경에서 비정상적인 게임 플레이를 위하여 사용되는 프로그램에 대하여 알아보고 게임 봇 탐지를 위한 다양한 연구 사례를 소개한다.

1. 서론

전용회선을 통해 고속 인터넷이 널리 보급되기 시작한 1996년 이후 국내 게임 산업은 급격한 성장세를 보이고 있다. 국내 게임 분야 총 매출을 보면 2003년 3조 9,387억원 규모에서 2011년에는 7조 4,312억원으로 하나의 지식서비스 산업으로 중요한 위치에 있다. 특히 온라인 게임이 차지하는 시장 규모는 4조 7,637억원으로, 국내 전체 시장점유율 64.2% 기록하였다. 또한 2011년에 조사한 국내 게임의 세계시장 점유 비율에서 온라인 게임 부분이 세계의 25.9%를 점유하고 있어 중국(30.4%)에 이어 세계 2위이다[1]. 이와 같이 온라인 게임 산업은 게임 산업 뿐 아니라 우리나라를 대표하는 산업 중 하나로 부상하였다.

다양한 종류의 온라인 게임 장르 중 MMORPG (Massive Multiplayer Online Role Playing Game) 장르는 2004년 이후 사람들에게 많은 관심을 받으며 시장성 면에서 두드러진 성장을 보여 왔다. 흔히 '대규모 다중 사용자 온라인 롤플레잉 게임'이라 불리는 MMORPG 장르는, 각 사용자들이 게임 속에서 마치 현실처럼 경제 활동, 사회 활동 등, 또 다른 하나의 사회를 구성하여 생활 할 수 있을 뿐 아니라 현실 속에서 경험하지 못한 일들을 경험할 수 있는 기회를 제공하고 있다.

하지만 이렇게 눈부신 발전의 이면에는 온라인 게임 플레이어의 피해 사례도 적지 않게 나타나고 있다. 2005년 대한민국 게임백서에서 조사한 설문조사 중 서비스 개발자 및 운영자들의 70%가 서비스 운영에 피해를 받았다고 응답하였고, 게임 서비스 사용자들 중 38.5%도 피해를 받은 경험이 있다고 답해 문제의 심각성을 보여주고 있다[3]. [그림 1]에서 보는 바와 같이 온라인 게임 해킹 툴의 발견 건수가 2008년에 506건, 2009년 상반기에 476건이라는 수치를 보이고 있다. 해킹 툴의 종류는 오토 플레이, 메모리 조작, 파일 조작, 패킷 조작, 스피드 핵 및 기타 등 총 6가지인데, 이 중에 메모리 조작과 오토 플레이는 각각 41%와 38%로서 온라인 게임 서비스 피해를 유발하는 대표적인 유형이다.



[그림 1] (좌) 온라인 게임 해킹툴 발견 건수, (우) 해킹 툴의 종류[6]

2. 온라인 게임에서 게임 봇(Game bot)

일명 '게임 BOT'이라고도 불리는 오토 플레이 프로그램은 미리 설정된 동작대로, 일반 사용자가 직접 조종하지 않아도 자동으로 사냥 및 채집활동 등 게임 내부의 활동을 한다.

오토 플레이 프로그램은 사람의 외부 조작 없이도 사람처럼 게임 환경 안에서 사용자에게 이득이 되는 활동을 지정한 기한까지 반복적으로 수행하며, 이를 사용하는 사람은 정당하지 못한 방법으로 이득을 얻게 되어 정상적으로 게임을 하는 일반 사용자에게는 상대적으로 피해를 주게 된다. 이와 같은 오토 플레이 프로그램의 무분별한 사용으로 인한 MMORPG 속 경제 붕괴 및 인플레이션 가속화는 일반 사용자들이 피해를 느끼고 게임을 떠나게 하는 원인이 되고 있다. 이 때문에 게임 완성도가 높은 MMORPG가 오토 플레이 프로그램의 폐해로 사용자가 거의 없는 유령 게임으로 전락하는 경우도 종종 발생한다. 이러한 문제는 MMORPG를 서비스 하는 회사뿐 아니라 게임 산업 전체를 위축시키는 결과를 초래하게 된다.

하지만 게임 오토 플레이 프로그램은 키보드 및 동작 입력과 같은 행동을 게임 플레이어와 동일하게 취하도록 설계 되므로, 메모리 조작을 방지하기 위한 클라이언트 영역의 보안 감시 방법으로는 검출이 불가능하다. 따라서 게임 서버 영역에서 게임 플레이어가 움직이는 행동을 수집/분석하여, 게임 플레이어가 일반 플레이어인지 오토 플레이 프로그램인지를 구별하는 방법만이 유일한 방법이다. 이에 일부 온라인 게임 서비스 업체에서는 일반 사용자의 신고를 받거나 온라인 게임 운영자의 모니터링을 통해 오토 플레이 프로그램의 사용을 발견하고 있지만 이 또한 역부족이다[4]. 그러므로 일반 사용자와 오토 플레이 프로그램과의 근본적인 차이점을 발견하고 이를 기반으로 한 오토 플레이 프로그램 사용 감지 및 검출에 대한 연구가 시급한 실정이다.

3. 게임 봇 탐지 기법 사례

국내의 경우 보안업체인 Inca Internet과 안철수 연구소를 중심으로, 동작중인 프로세스를 분석하는 연구가 상대적으로 많이 진행되고 있다[5][6][7].

국외의 경우 게임 내에서 사람만이 반응 가능한 조건을 생성하거나, 이동 경로를 분석하는 등 게임 내적 요소의 분석을 통해 오토 플레이 프로그램의 사용을 검출해 내고 있다[9][10][11]. 이는 국내 연구에 비해 향상된 연구로 볼 수 있으나, 특정 게임 장르에 의존적 혹은 검출을 위한 비교 요소에 대한 정의가 미흡한 편이다.

봇 탐지를 위한 기술 요소를 살펴보면, 오토 플레이 프로그램을 감지하고 대응하는 기술로서 하드웨어 기반의 방법, 게임 튜링 테스트, 캐릭터의 경로 기록 사용, 클라이언트 컴퓨터의 메모리 분석 등 다양한 방법을 연구하고 있다. 하지만 이와 같은 기술들은 감지 원리가 알려지면 이를 피할 수 있는 방법을 쉽게 고안할 수 있다는 한계가 있다.

3.1. 국내 연구 사례

- GameGuard (Inca Internet)[5] : 알려진 불법 프로그램의 정보를 수집하고 이를 이용하여 수행 중인 프로세서가 불법 프로그램 여부를 파악하는 것으로 프로그램의 불법적 조작을 방지한다. 단점으로 알려지지 않는 불법 프로그램은 검출해내지 못함 감지 프로그램이 반드시 실행 중이여야 하기 때문에 감지 프로그램을 종료시키거나 실행을 방해하는 방법으로 감지 회피가 가능하다.
- 리니지 2(NC Soft) : 리니지2 게임 접속자의 행위 로그를 수집하여 오토 플레이 프로그램 사용자의 계정을 차단한다. 오토 프로그램 사용자의 검출 방법은 공개되지 않았으며, 사용자의 행위 모델과 오토 프로그램의 모델 비교가 아닌 단순 로그 분석을 통한 검출로 예상된다.
- Detection of Auto Programs for MMORPGs(동국대학교)[7] : 사람과 오토 프로그램의 키보드와 마우스 입력 정보 수집 후 분석을 통하여 오토 플레이 프로그램을 검출한다. 오토 프로그램의 키보드와 마우스 입력이 사람보다 많다는 점을 이용하여 오토 프로그램을 검출한다. 오토 프로그램의 설정 변경을 통하여 입력을 줄일 수 있으므로 근본적인 해결 방법이라고 보기 어렵다.
- Hack Shield(안철수 연구소)[6] : Inca Internet의 GameGuard와 유사한 기능을 제공하며 단점도 유사하다.

3.2. 국외 연구 사례

- 테스트 소프트웨어를 이용한 게임 봇 방지 기술 (Palo Alto Research Center) [9] : 온라인 게임 내에서 작동하는 게임 튜링 테스트를 사용하여 게

임 봇을 검출하는 방법을 연구하였다. 기존의 방지 방법이 일반 사용자와 봇 사용자의 구분이 명확하지 않을 경우 일반사용자에게도 피해를 줄 수 있기 때문에 사용자가 게임을 하는 동안 사용자에게 특정 문제를 주어 일반 사용자임을 확인하는 Turing Test 테스트를 제안하였다. 사용자가 게임을 플레이하는 동안에 테스트가 진행되기 때문에 사용자로 하여금 게임에 대한 재미를 반감시킬 수 있는 문제점을 안고 있다.

- 행동 기반 치팅 사용자 검출 기술 (University of York) [10] : 게임 내 치팅 (Cheating) 사용자의 불법적 접근을 검출하기 위한 목적으로 사용자의 행동을 모델링 하여 불법적 접근 유형을 정의하고 이를 통해 치팅 플레이를 판별한다. 연구의 기반 분야가 1인칭 슈팅 게임으로 한정되어있어 다른 게임 분야에 적용되기 어렵다. 행동 요소로서 게임 내 캐릭터의 이동 경로 데이터만을 사용해 치팅 사용자를 검출하기 때문에 보다 다양한 행동 패턴을 보이는 치팅 사용자 검출에 있어 그 한계성을 보이고 있다.
- 하드웨어 기반 치팅 방지 기술 (Portland State University) [11] : 게임 클라이언트에서 동작하는 속임 방지 (Anti-Cheating) 방법이 데이터 변조 방법을 통해 충분히 피해 갈 수 있다는 점에 착안하여 하드웨어적으로 접근하는 방법을 사용하였다. 하드웨어를 기반으로 치팅 프로그램을 제한하여 오토 플레이 프로그램이 가지고 있는 근본적인 문제를 해결한다는 점에서 새로운 기술이라고 볼 수 있으나 하드웨어적 접근은 가격 면에서나 제약조건이 심하다는 문제점을 안고 있다.

4. 결론 및 향후 연구

봇(Bot) 프로그램의 사용 방지를 위한 방법으로 게임 클라이언트 영역에서 해킹과 함께 오토 플레이 프로그램을 감지하는 연구들이 진행되고 있다. 그러나 이러한 연구의 대부분은 게인 사용자의 PC에 설치되어 감시를 하기 때문에 오토 플레이 프로그램 제작자들에 의해 변조되어 감시가 불가능하게 되는 한계성을 가지고 있다. 이와 같은 문제를 방지하기 위해 게임 서버 영역에서의 오토 플레이 프로그램 감지 방법이 필요하다. 또한 만약 감지 방법을 알았다고 해도 피할 수 없도록 오토 플레이 프로그램 가지는 한계성을 연구해 고유의 특징 점(Feature)을 발견하고 이를 통한 오토 플레이 프로그램 감지를 수행하는 연구가 필요하다.

감지 기술을 통해 오토 플레이 프로그램을 식별했다 하여도 실제로는 그 플레이어에게 제제를 가하는 것은 매우 신중해야 한다. 이는 잘못된 식별 결과로 일반 플레이어에게 제제를 가했을 경우 서비스를 제공받는 플레이어의 입장에서 매우 큰 피해에 해당하기 때문이다. 따라서 확실한 오토 플레이 프로그램 식별을 위하여, 검증 방법을 이용한 명확한 오토 플레이 프로그램 검출 기술이 필요하다.

향후에는 게임 봇 검출을 위한 게임 로그 데이터의 수집과 분석을 위한 알고리즘 개발, 그리고 실시간 온라인 게임에 다시 적용하기 위한 방법이 요구된다.

참고문헌

[1] 한국콘텐츠진흥원,“2011 대한민국 게임백서”, 2011.
[2] 게임전문리서치 게임트릭스, www.gametrics.com.
[3] 장항배, 김경규, 이시진, “게임 서비스 침해유형에 따른 기술적 대응방안 연구”, Information Systems Review, Vol.9, No.3, 2007.
[4] 한국 정보보호 진흥원, 온라인 게임 해킹 대응 가이드, 2006.
[5] Inca Internet, www.inca.co.kr
[6] 안철수연구소, www.ahnlab.co
[7] H. Kim, S. Hong and J. Kim, “Detection of Auto Programs for MMORPGs,” Springer, AI 2005: Advances in Artificial Intelligence, pp.1281-1284, 2005
[8] 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,” Proceedings of the ACM SIGCHI Conference, 2006.
[9] Philippe Golle, Nicolas Ducheneaut, “Preventing Bots from Playing Online Games,” Computers in Entertainment (CIE), vol. 3, 2005.
[10] W. Feng, E.d. Kaiser, T. Schluessler, “Stealth Measurements for Cheat Detection in On-line Games,” Proceedings of the 7th ACM SIGCOMM Workshop on Network and System Support for Games, pp.15-20, 2008.
[11] P. Laurens, R.F. Paige, P.J. Brooke and H. Chivers, “A Novel Approach to the Detection of Cheating in Multiplayer Online Games,” 12th IEEE International Conference on Engineering Complex Computer Systems, pp.97-106, 2007.