Bots Problem in Online Games

Dewanshu Jain, Alok Gupta

Abstract: In this paper discussion about the bots issues in online games which is a serious threat to the online games business and causes a huge revenue loss to the industry has been highlighted. The behavior of bots, present security mechanisms and the shortcomings of existing technologies has been reviewed and some suggestions to improve the security against bots have been purposed.

Keywords: Bots, games, mechanisms, technologies.

I. INTRODUCTION

The growing progress in computers in every field has made computers very popular in every field one such field in the entertainment. Earlier entertainment includes Movies, Music and some of the computer games. But with the advancement of internet some new sources of entertainment came into existence such as chatting, online music, videos and mainly online games. Online games made a tremendous progress in a very short span of time. Playing game online with human opponents was one of the major reasons why the players loved this type of game and some games also provide a facility to chat within games which adds to fun in the game. Many gaming companies have made huge profit through online gaming business, one such game is World of Warcraft(WoW) which made a tremendous profit in online gaming industry. The market leader alone—Blizzard Entertainment's World of Warcraft (WoW)—surpassed 11.5 million subscribers in December 2008, making in an estimated US$150 million in subscription fees per month et al.[1]. Now when the gaming companies make such huge revenue from the game, it becomes a duty of the game provider to satisfy the customer. One of the threats to the game providers is cheating in online games. The definition of cheating says "the execution of some action that is out of the normal games methods or contest with the expectation or hopes that this will bring some advantage to the game" et al.[2]. One way of cheating in online games is by using bots. "Game bot is the tool which is used for the game cheating. Players can gain an advantage out of the context of the game rules' permission, or achieve the target easily which honest players need longtime effort to get."et al.[3]

II. MOTIVATION

The question that first comes to our mind is why players use bots? There are different reasons for this. The first reason is to earn maximum gold. When we play the game we make points by hitting the enemy or by completing certain task in the game, this process is also known as gold farming. The players make gold in order to buy the virtual products in the games which makes their avatar stronger. Some players also make profit by selling the virtual products to some other players in exchange of real currency. In 2009, games played on social networks such as Facebook, games that primarily derive revenue from the sale of virtual goods, brought in 1 billion USD, and that is expected to increase to 1.6 billion in 2010. Worldwide, 7.3 billion USD was made from virtual goods that same year.et al. [4]. So in order to make maximum game currency with minimum labor the players use bots moreover a part of game could be boring and repeating again and again so the players use bots to skip that part and jump to next round. The other reason is as bots require no human intervention so they can run automatically again and again, so that player can make hefty points by playing the game for 24 hours without getting fatigue. When some players make too much game currency by using the bots in the online games the price of the online virtual items in the game increases as a result the interest of the honest players who play the game in a fair way decreases and switches to some other games or stop playing that game. Which decreases the number of players playing the game hence it leads to the loss of revenue to the game developers which demotivates the game developers to further invest in the online gaming industry as a result this industry faces set back.

III. TERMINOLOGY

The word "bot" comes from the robot which does all its work automatically. In context of online games the "Bot" is a program that automatically plays the game with minimum or zero human effort. A bot is artificial intelligence expert system software which for each instance of the program controls a player. These programs automatically run without any human intervention or very little human effort and keeps on killing a large number of enemies as a result of it the player can kill a large number of enemies and earn a lot of points. Bots are broadly of two main types et al.[5]

- **Static bots** are designed to follow pre-made waypoints or path nodes for each level or map. These bots need to have a unique waypoint file for each map, or a path node system embedded in the map, if they are to function. For example, Quake 3 Arena bots use an AAS (area awareness system) file to move around the map, while Counter-Strike bots use a WPT (waypoint) file.
- **Dynamic bots**, on the other hand, dynamically learn the levels and maps as they play. RealBot, for Counter-Strike, is an example. Some bots are designed using both static and dynamic features.

Manuscript Received on July 2014.

Dewanshu Jain, Assoc. Business Analyst, Xerox Services, Xerox, Gurgaon, India.

Alok Gupta, OSS-RC Engineer, Ericsson India Global Services Pvt. Ltd., Gurgaon, India.

Gold farming a process in which the players makes the maximum points or makes gold by playing the game again and again or killing large number of enemies they gain certain points which helps them to get some reward which makes their character better et al[6]. People in China and in other developing nations have held full-time employment as gold farmers. While most game operators expressly ban the practice of selling in-game currency for real-world cash, gold farming is lucrative because it takes advantage of economic inequality and the fact that much time is needed to earn in-game currency. Rich, developed country players, wishing to save many hours of playing time, may be willing to pay substantial sums to the developing country gold farmers.

IV. ANALYSIS OF ANTI-BOT MECHANISM

Following are some of the measures that are provided to check the online bots.

A. Players Reporting and GM Patrolling

In et al.[7] the author proposed a process in which if a player playing online games, when find someone suspected cheating then they report to the game master (GM). When GM receives the report the GM checks if the player is playing according to the rules or not if any suspicious activity is received then the account of the player is blocked. The GM also performs the petrol in the game and looks for the bots or players who cheats in the game and freeze their accounts. But since the number of players are lot more than the number of GM so it`s very difficult for GM to detect all the bots moreover some bots follow the human like behavior.

B. Improve Packet Encryption

In view to cheaters can find the encryption schemes of the packets, the game operators need to make some more complex algorithms for packet encryption in order to make it difficult for cheater to understand. But this technique also have drawback as the more time would be required and more resources would be required to deal with data. As a result the player would not be able to experience the realistic experience. And more over this packet cannot prevent the packet to be cracked et al.[8].

C. Monitor by Server

Once finding suspicious behaviors, servers will compares against known cheat code. GM will freeze the cheaters account if data matches with cheat code. As the number of game players increasing, servers need deal with more data and kinds of game bots. Heavier burden for servers might affect the game quality et l.[9].

D. CAPTCHA Test

The player will see a text in the image and he will need to enter the text in the image, in case he is able to enter the correct text he is authorized to play the game. But this mechanism fails the smooth function of the game. Moreover the player can use the image reorganization software's et al.[10].

E. Embed Monitoring Tool in Client

In this we use some tools that uses tools that detects for suspicious software`s that are running on the client computer including memory, game process space, DLLs running in that space and so on. Some tools even do things like reading the window text in the title bar of every window and doing a scan of the code loaded for every process running on your computer to check the bots. But these software`s compromises with the clients privacy moreover these are stopped by the anti-viruses. Furthermore cheater can use more advanced hack technology to invade them et al. [11].

F. WoW Alyzer

In et al.[1] the authors purposed an approach in which, when a player moves his or her character in a virtual world, the game client regularly sends packets with new coordinates to the server. Hence, the movement coordinates readily variate on the server side. The first approach is to log the character's movement and use this game trace. In this way, we eliminate dot clusters that occur when multiple packets arrive in quick succession at the same location for example, to update the rotation when the mouse turns a character. The simplification helps the waypoint extraction algorithm concentrate on areas where the dots accumulate because the character passed that point several times. In this the researchers calculated the number of times the player passes through the same segment. The main difference between human player and the bot was that the bot player follow the same path again and again hence bots go through the same segment repeatedly while the humans are adventurous and try to do new things and also there is no chances that a human can follow same segment paths again and again because there is always a variation when human play a game.

A.Human Observation Proofs(HOPs)

It differentiate bots from human players by passively monitoring input actions that are difficult for current bots to perform in a human-like manner et al.[12]. The talk describes a prototype HOP-based game bot defense system that analyzes user-input actions with a cascade-correlation neural
network to distinguish bots from humans.

B.NEO Protocol

In et al[13] the author proposed a protocol that divide the time into the uniform time intervals, called rounds, in which each player sends its update all the other players. Each update is encrypted and a key with which they are encrypted is exchanged between the players. Rounds are used by players to send their updates with the most delays, because late updates will be ignored. Following cheats are avoided with this technique:

- Delay Cheat: Avoid this cheating through limited size round. Late updates are ignored.
- Inconsistency cheat: NEO avoids inconsistency cheat by using digital signatures, Players audit the

- game state, and when two of them discovers different states, the packages received are used how cheating evidence.

C.Neural Network Approach

In et al.[14]The choice of Artificial Neural Networks (ANN) was made because their great capacity to pattern recognition and generalization, where the network after trained, can recognize patterns that were off the training step. Accordingly a brief study, two ANNs architectures were chosen the Multi-layer Perceptron (MLP) and a time delay architecture, the Focused Time Lagged Feedforward Network (FTLFN). Data to be analyzed by the ANN, is related to the processed information send by the participants, where there are linear and angular velocities in three axes (X, Y and Z), energy variable (amount of energy that one virtual hover has) and turbo variable (informing if hover can run faster or not). Even with the ANN approach, the system will remain with the passive reaction that means, the client's machines will report their results to the server, where a judge will just take an action accordingly the relevant information sent.

V. FLAWS IN CURRENT ANTI-BOTS SYSTEM

Although the techniques we have read are quite useful for the defense but yet these are not enough to stop the bots from entering the online games. The first reason is there is no standard definition for online "Game Bots". The second reason is there are many different games and different bots are designed for different games so the approach we use for one game may not be applicable for the other game. The third reason is bot maker keeps on using up to date technology for making bots which makes us difficult to identify the bots in the online games. There is a lack of laws and punishments for the people who are found culprit of cheating in the games. The last reason for this is lack of game security is different from other tradition techniques of security used over internet. So it is not too much explored yet, a large party of this study is yet to be touched so it will take time to develop an extremely secured system.

VI. CONCLUSION

As we see that online games are becoming extremely popular these days, yet the security issue is a big concern for them. Although many security mechanism exist but still they are not sufficient to stop the bots in the online games. The game developers and the service providers should invest more in the game security and a strict action must be taken against those people who are found culprit of cheating. This area still lacks in research so more emphasize should be given on the up to date anti bots mechanisms. So our future work is to develop an anti bots system which can detect bots in the games, so that the proper action can be taken against them.

REFERENCES

1. Mitterhofer, Stefan, Christopher Kruegel, Engin Kirda, and Christian Platzer. "Server-side bot detection in massively multiplayer online games." Security & Privacy, IEEE 7, no. 3 (2009): 29-36.
2. Gaspareto, Otavio Barcelos, Dante Augusto Couto Barone, and André Marcelo Schneider. "Neural networks applied to speed cheating detection in online computer games." In Natural Computation, 2008. ICNC'08. Fourth International Conference on, vol. 4, pp. 526-529. IEEE, 2008.
3. Xiao, Lan, Zhang Yi-Chun, Yang Cheng, and Zhang Ming-Kai. "An Investigation of Online Game Bots in China." In E-Product E-Service and E-Entertainment (ICEEE), 2010 International Conference on, pp. 1-5. IEEE, 2010.
4. As listed on the website of Wikipedia "http://en.wikipedia.org/wiki/Virtual_goods".
5. Wu Chun, Zhu Guo-hun, Wu Yong-hua1, Xiang Rong. "The Study of Bot Technology for Online Games" IEEE
6. R. Heeks, "Current Analysis and Future Research Agenda on 'Gold Farming': RealWorld Production in Developing Countries for the Virtual Economies of Online Games," Working Paper Series, vol. 32, 2008. www.sed.manchester.ac.uk/idpm/research/publications/wp/di/di_wp32.htm
7. K. Warns, "Cheating Detection and Prevention in Massive Multiplayer Online Role Playing Games", The Seventh Annual Winona Computer Acience Undergraduate Research Symposium,Winona, MN, pp.26-30, April 2007.
8. J .Yan and H.J. Choi, "Security Issues in Online Games", The Electronic Library, MCB, UP, Ltd,Vol. 20, No.2, pp. 125-133, 2002.
9. P. Golle, N.Ducheneaut, "Preventing bots from playing online games", Computers in Entertainment, Vol.3(3), New York, ACM, pp.3-12, July 2005.
10. Philippe Golle , Nicolas Ducheneaut, Keeping bots out of online games, Proceedings of the 2005 ACM SIGCHI International Conference on Advances in computer entertainment technology, Valencia, Spain, pp.262-265, June 15-17, 2005.
11. Kuan-Ta Chen , Andrew Liao , Hsing-Kuo Kenneth Pao , Hao-Hua Chu, "Game Bot Detection Based on Avatar Trajectory", Proceedings of the 7th International Conference on Entertainment Computing, Pittsburgh, pp.94-105, September 25-27, 2008
12. Gianvecchio, Steven, Zhenyu Wu, Mengjun Xie, and Haining Wang. "Battle of Botcraft: Fighting Bots in Online Games with Human Observational Proofs." (2009).
13. GauthierDickey, Chris, Virginia Lo, and Daniel Zappala. "Using n-trees for scalable event ordering in peer-to-peer games." In Proceedings of the international workshop on Network and operating systems support for digital audio and video, pp. 87-92. ACM, 2005.
14. Gaspareto, Otavio Barcelos, Dante Augusto Couto Barone, and André Marcelo Schneider. "Neural networks applied to speed cheating detection in online computer games." In Natural Computation, 2008. ICNC'08. Fourth International Conference on, vol. 4, pp. 526-529. IEEE, 2008.

AUTHORS PROFILE

Mr. Alok Gupta, Currently Working as an OSS-RC Engineer at Ericsson India Global Services Pvt. Ltd., Gurgaon, India, he is looking after the OSS-RC for Customer Support dept. of EGI for Various Network Technologies like GSM/GPRS/CDMA/3G/LTE nodes. Before Ericsson, he was working with HCL Technologies Ltd. – IOMC as a Specialist-Unix Operations and managed various UNIX servers for various Clients of HCL. He had done Bachelors of Technology (Hons.) i.e. B.Tech in Computer Science Engineering in 2011 from Lovely Professional University, Punjab, India.

Following are the Honors and Awards he achieved till now at various levels,

Guest of Honor at Lovely Professional University | February 2014
Attended Alumni Guest Lecture Series and interacted with final and pre-final year students of University.
Certificate of Appreciation at HCL Technologies Ltd. | October 2013
Certificate of Appreciation from EFH-DC Department/OMC for being a quick learner
O2 League Membership at HCL Technologies Ltd. | July 2013
Scored outstanding rating from last two years at HCL Technologies Ltd
Star performer at HCL Technologies Ltd. | January 2012
Be the Star performer at HCL Technologies for the month of January 2012
Comnet Jewel at HCL Technologies Ltd. | December 2011
Be the Comnet Jewel at HCL Technologies for the month of December 2011.
University Honor Roll at Lovely Professional University | March 2011
Be the University Honor Roll for the year 2009-2010.
For more detail about him, you can go through his LinkedIn profile, *in.linkedin.com/in/alokgupta89/.*

Mr. Dewanshu Jain, Currently Working as an Associate Business Analyst at Xerox India Services Pvt Ltd., Gurgaon, India, he is looking after the the Manual and Automated Testing of various systems for clients. Before Xerox, he was working with Aon Hewitt India Pvt Ltd as a Senior Setup Configuration Specialist and involved in the Validation and Verification phases for various for various ongoing and implementation clients of Aon Hewitt.. He had done Bachelors of Technology (Hons.) i.e. B.Tech in Computer Science Engineering in 2011 from Lovely Professional University, Punjab, India.
Following are the Honors and Awards he achieved till now at various levels,
Ingenious Heads at Aon Hewitt India Pvt Ltd| January 2014
Implementing Idea on one of my clients which was replicated in many other client and saved cost for the organization.
Benefits Wizard at Aon Hewitt India Pvt Ltd| September 2013
Awarded for leading the project and coordinating with onshore requirements team and implementing the project with high quality even after getting requirements changed before 2 week prior to going live.
Tier 2 award at Aon Hewitt India Pvt Ltd. | July 2013
Awarded for great feedback from the onshore team about the ownership of projects and quality of work.
Platinum Team Award for year 2012. | January 2013
Our Team of 6 has implemented a project for ongoing client worth $11mn with high quality and without affecting ongoing deliverables.Client was amazed with the quality of the project implemented.
Tier 2 Award at Aon Hewitt India Pvt Ltd. | October 2012
Awarded for High quality deliverables within limited time and high quality of the Project delivered.
Maths Topper across the region in 10th Standard ICSE exam| May 2005
For more detail about him, you can go through his LinkedIn profile, https://www.linkedin.com/pub/dewanshu-jain/75/ba0/776