A Study of Various Bot Detecting Techniques in Massively Multiplayer Online Games

[1]Gagandeep Singh, [2]Vikrant Sharma
[1]Anand College of Engg. & Mgt., Kapurthala, Punjab, India
[2]CT Institute of Technology, Jalandhar, Punjab, India

Abstract
In this paper we study various techniques that are used to detect the bots in Massively Multiplayer Online Games (MMOGs). We discussed how these techniques work and how they were successful in detecting bots in online games and the flaws in these techniques and about the future scope in this field.

Keywords
Bots, MMOGs, Goldfarming

I. Introduction

In modern era of computer world the trend of computer games as a source of entertainment is gaining a massive popularity. With improvement in communication through internet technology, the games were played over internet making players to compete against one another. 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.[1]. 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.[2].

But this technology also faces a huge challenges in market. Players are looking for unfair ways to complete the take. One such problem faced in online game market is the problem of bots.

II. Terminology

In such games the player is given a certain task and after completing that task successfully he earns some points, by using these points he can purchase products from game market and make his character better. The other way through which he can make his character stronger is by purchasing those products by paying certain amount of money (real currency). So in order to make their characters better ether the player have to play the game for a long time or he have to buy the products in exchange of real money from the market. There are some players in the game who writes a program that controls the moment of the character in online games. The word bot is derived from last three letters of the word "Robot", a robot is a machine that automatically performs a certain task with a very little or without any human effort. Similarly in the terms of Massively Multiplayer Online Games (MMOGs), a "bot" is a program that plays the game on the behalf of human, with zero or very little human effort. These were known as bots, these bots read the game map from the game memory and takes the action accordingly without any human effort. The bot programmer use bot to make points then purchase goods from game market and sell them for a little less price than the game price and in this way earns money in real.

Bots are broadly classified into two main categories et al [3]:-

1. Static bots are designed to follow pre-made way points 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.
2. Dynamic bots, on the other hand, dynamically learn the levels and maps as they play.

Gold Farming

There are people who play the game for a long time and make many points because of their great skills and more time they can devote to game and hence can buy products in games. They sell these products to other players at a price less than the price of the product in the game. Such players are known as gold farmers and the process is called gold farming. In other words, gold farming is 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 [4].

III. Various Approaches to Detect Bots in Online Games

Many scientist from all over the world are working to find out various techniques to prevent bots in online games. Some of the techniques are as follow:-

A. Anti-Hook Technique

The hook technique basically works with the Direct Link Libraries (DLL), when a player plays an online game, the DLL files are loaded from the client computer to the server. The programmer writes a bot program in one such DLL file, when this file gets loaded into server computer, the bot program in DLL file gets loaded and hence the bot is inserted into the online game. Fig. 1 shows how a bot program written in client machine gets loaded into server side.

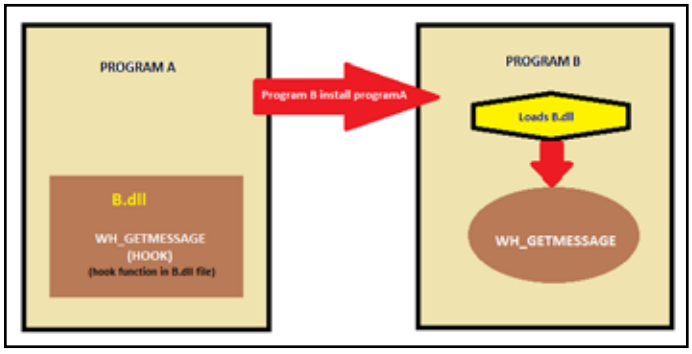

Fig. 1: How Hook Invades a Process

Anti-global Hook technology

In this technology author follow the following steps et al.[5]:-

1. Author made a new library function newLoadLibraryExW whose prototype is same as LoadLibraryExW. All functions that call LoadLibraryExW must pass through newLoadLibraryExW.
2. A block of space is provided. If initial address of the space is fakeLoadLibraryExW, we store the first N bytes of the function LoadLibraryExW, and then hold on the running program by using an instruction jump back address LoadLibraryExW.

3. The front five bytes of function LoadLibraryExW is modified, and then use an instruction jump to jump function newLoadLibraryExW.

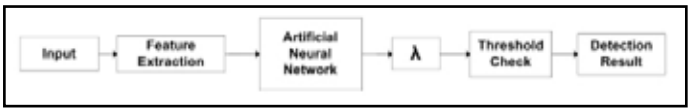

Fig. 2: Shows Working of Artificial Intelligent System et al.[6]

B. Artificial Neural Network Approach

The choice of Artificial Neural Networks (ANN) was made because their great capacity to pattern recognition and generalisation, where the network after trained, can recognize patterns that were off the training step. There are two main actions that are taken into consideration. The first is the moment of the player in the virtual world and the next is the set of actions that are taken by the player to fight against a certain enemies. These features are extracted and are put into an Artificial Neural Network system. The output of ANN based on moment is (λ1) and action is (λ2) and are named as confidence level for each type and values between 0 and 1. "0" indicates that error is rate is high so current player is human while "1" indicates error rate is low and player is a bot. The process is described in fig. 2 et al [6].

C. Human Observation Proofs (HOP)

In Human Observation Proofs methods we recognize the behavior of the various players playing online game, the player which shows a different or unnatural behavior is classified as bot. The behavior of bots is different from those of humans. The bots are detected through their unexpected behavior. 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.[7]. The HOP system consists of client-side exporters and a server-side analyzer. Each client-side exporter collects and sends a stream of user-input actions taken at a game client to the game server. The server-side analyzer then processes each input stream and decides whether the corresponding client is operated by a bot or a human player et al.[8].

D. Human Identification Proofs (HIP)

In Human Identification Proofs (HIP) method we use some software or some tool which is put forward before the person enters the game. The person has to pass the tool test in order to enter the game arena. The example is CAPTCHA is Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA). In this technique an image is shown it have some jumbled text in it, the player have to enter the text as in the image, if the person enters the correct text then he can enter in else not. A CAPTCHA sample is shown in fig. 3.

Fig. 3: Sample CAPTCHA

E. Statical Aimbot Detection System

Aimbot is the aiming robot. The work of aimbot is to aim at the enemy automatically. The aimbot users aim much better that the average players. The aimbot has access to games internal state so it can acquire the target as soon as there is a direct line of sight between player and target. So the players using aimbot acquires target with both speed and accuracy moreover it has more efficiency than the normal players. For a normal player it is impossible to get this speed and accuracy for an instance consider if the target is just behind the user for a normal human player it will be difficult to immediately recognize where the target is moreover he will take time to rotate at the angle of 180 degree and hence find a target and shoot at it, but in case of aimbot, the bot automatically knows where the target is from the internal game states data, hence it quickly turns and locks the target even if it is at the back in a fraction of time. Thus abilities of human like accuracy, speed, map reorganization and spatial awareness etc does not come into consideration. Two features were taken to measure the performance of the player.

1. Cursor Acceleration When Acquiring Aim (AccA)

This feature monitors the speed of cursor when acquiring a target, it checks the time taken by the player to lock the target. As aimbots are quick and fast they can easily read internal game data and hence know the position of the target even if it is very far away from the player even if it is not even in the sight or even if it is directly behind the player. For normal human player it takes time to detect the position of the target and it takes time for a normal player to detect the target.

While the aimbot is much fast and it locks the target quickly no matter how far it is or even if is directly behind player as a result speed to lock target, reflexes and accuracy is much higher from humans et al [9].

This feature is calculated by first calculating the displacement caused by mouse to aim at target, and the acceleration.

- Yaw: - Angle on horizontal plane (influenced by left right movement of mouse).
- Pitch:-Angle on vertical plane (influenced by up down movement of mouse).
- Roll:-The rotation of viewpoint on horizontal plane (influenced by moment of mouse).

Euclidean distance was used to calculate the change to pitch and yaw (players aim) from its previous frame

$$\sqrt{(\Delta Yaw)^2 + (\Delta Pitch)^2}$$

Where Δ is the difference of angles between time t and t-1. Et al [9].

The mouse sensitivity was not measured by using windows events because different players may have different mouse sensitivity et al [9].

2. Time of Target (ToT)

This feature shows how long a player can lock a target. As the aimbot can lock target for a long time while a normal human it depends on their skill and moreover they can`t lock target for long time. This feature is calculated by tallying number of frames in duration of targeting event et al [9].

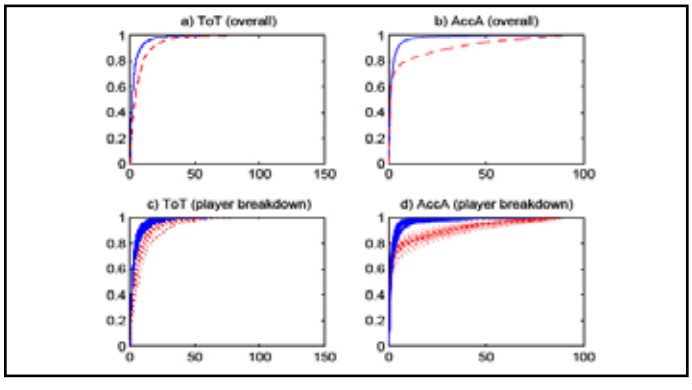

Fig. 4: Shows the Result of Tot and AccA et al.[9]

The above diagram shows Empirical Cumulative Distribution Functions (ECDF) of features. With fig 1 (a and b) showing overall ToT and AccA respectively while, and fig. 1 (c and d) shows same for indusial players.

IV. Flaws in Present Mechanisms

The major drawbacks of our present mechanism is that our present mechanisms are not yet perfect, sometimes a human player is wrongly classified as bot and hence it causes frustration for them as a result of it the normal human player gets frustrated and hence leaves the game.

Lack of capital punishments against the bot user encourages the bot users to use bots without any fear.

Sometimes bots shows more human like behavior as a result it becomes extremely tough to identify the bots.

The speed will be effected in order to scan all .dll files as each file will be scanned before the game is loaded in the server side.

The artificial neural network is good in its own way but to use this approach we need to have a different artificial intelligent system for different games and moreover it is very hard to collect data from a large pool of population and built a system that can give result with exact accuracy and there are many chances for bots to be classified as humans and vice versa.

There are various software's that are used in order to break the CAPTCHA so using it does not provide a complete security.

The aimbot detection system is not good enough when the players have great skills in playing game, there are chances that the players with better skills can be classified as bots in this system.

V. Conclusion

In this paper we discussed about various methods that were used in order to detect bots in online games. Although these methods were very good up to certain extinct but yet we lack in tools that may help us to completely stop bots from playing online games. More strict laws should be made against the culprits using bots and more work has to be done in this field in order to stop bots in playing online games.

References

[1] Wikipedia. (June 2013). [Online] Available: http://www.en.wikipedia.org/wiki/Virtual_goods

[2] Mitterhofer, Stefan, Christopher Kruegel, Engin Kirda, Christian Platzer,"Server-side bot detection in massively multiplayer online games", Security & Privacy, IEEE 7, No. 3, 2009, pp. 29-36.

[3] Chun, Wu, et al.,"The Study of Bot Technology for Online Games", Genetic and Evolutionary Computing, 2009. WGEC'09. 3rd International Conference on. IEEE, 2009.

[4] 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.

[5] Chun, Wu, et al.,"The Study of Bot Technology for Online Games", Genetic and Evolutionary Computing, 2009. WGEC'09. 3rd International Conference on. IEEE, 2009.

[6] Platzer, Christian,"Sequence-based bot detection in massive multiplayer online games", Information, Communications and Signal Processing (ICICS) 2011 8th International Conference on. IEEE, 2011.

[7] Lyhyaoui, Y., A. Lyhyaoui, S. Natkin,"Online games: Categorization of attacks", In Computer as a Tool, 2005. EUROCON 2005. The International Conference on, Vol. 2, pp. 1340-1343. IEEE, 2005.

[8] Prasetya, Kusno, Zheng da Wu,"Artificial neural network for bot detection system in MMOGs", In Proceedings of the 9th Annual Workshop on Network and Systems Support for Games, pp. 16. IEEE Press, 2010.

[9] Yu, Su-Yang, et al.,"A statistical aimbot detection method for online FPS games", Neural Networks (IJCNN), The 2012 International Joint Conference on. IEEE, 2012.

Er. Gagandeep Singh is a student of M. Tech in Punjab Institute of Technology, Kapurthala, Punjab, India. His area of interest is network security. He is also involved in teaching and works as an Associate Prof. at Anand College of Engg. & Mgt., Kapurthala, Punjab, India.

Prof. Vikrant Sharma is currently serving as an Associate Professor in Department of Electronics and Communication Engineering, CT Group of Institutions, Jalandhar, India. His area of interest is optical fiber, micro-wave engineering and communication system. He is involved in teaching and research for than a decade. He is pursuing PHD in PTU Jalandhar.