Integrating Players, Reputation and Ranking to Manage Cheating in MMOGs

Dmitri Botvich
TSSG
Waterford Institute of
Technology, Ireland

Jimmy McGibney
TSSG
Waterford Institute of
Technology, Ireland

Georgy Ostapenko
TSSG
Waterford Institute of
Technology, Ireland

Stefano De Paoli
Dept of Sociology
National University of
Ireland, Maynooth

Aphra Kerr
Dept of Sociology
National University of
Ireland, Maynooth

Max Keatinge
Dept of Sociology
National University of
Ireland, Maynooth

ABSTRACT

In this paper, we propose an approach that uses in-game reputation as a solution to the problem of cheating in massively multiplayer online games. What constitutes cheating is however quite context-specific and subjective, and there is no universal view. Thus our approach aims to adjust to the particular forms of cheating to which players object rather than deciding a priori which forms of cheating should be controlled.

The main feature of our approach is an architecture and model for maintaining player-based and context-appropriate trust and reputation measures, with the integration of these into the game's ranking system. When an avatar loses reputation, our approach intervenes to reduce its ranking. It is envisaged that players will come to attach value to reputation in its own right. We also present the results of relatively large-scale simulations of various scenarios involving sequences of encounters between players, with an initial implementation of our reputation and ranking model in place, to observe the impact on cheaters (and non-cheaters).

Keywords

Massive multiplayer online games, cheating, reputation, trust.

1. INTRODUCTION

Massively Multiplayer Online Games (MMOGs) are a highly successful sub-sector of the digital games industry whereby players participate in a virtual world [1, 2] which is persistent, meaning that it runs independently of the user and requires continuous support from the game developer. MMOGs are both highly sophisticated technological systems - in most cases built around a client-server architecture - and 'deeply social' worlds [3, 4, 5] in which millions of players chat, cooperate, interact, compete and trade with each other online

through their avatars. Notable examples of these types of games are *World of Warcraft* (WoW) or *Lineage.*

In this paper we lay the foundation for an approach that uses in-game reputation as a solution to one of the problems that affects MMOGs, including role-playing games: cheating. We consider cheating in MMOGs as the group of actions that provide cheaters with unfair advantages over other players. Empirical studies of game play have shown that cheating in MMOGs is a highly contested and variable practice. It deserves particular attention because it is often perceived by the developers, publishers and some players to be a threat to the social experience, economic viability and security of a game world [6]. For others, cheating is viewed as justifiable because it offers the potential to generate large amounts of real and virtual money, or to progress more easily in the game rankings. By using a context sensitive and player-driven strategy, we propose an approach that aims to adjust to the particular forms of cheating to which players object, rather than deciding a priori which forms of cheating should be controlled.

The main idea of our approach is that the proper integration of a player-based and context-appropriate reputation mechanism into the game's ranking systems can lead to a sustainable solution to the problem of cheating. In this paper we describe the motivation for adopting such an approach and we also formalize an approach for the integration of the game rankings with a reputation system. With our approach it will become possible to use the reputation system to detect cheaters and mitigate the unfair advantage obtained. Speifically, we try to intervene in the ranking of the avatars belonging to cheaters within a game, where we consider ranking as a value that reflects the level of the in-game persona or avatar. Our approach intervenes by reducing the ranking of an avatar, when this avatar has a negative reputation (i.e. it is rated by the large player community as a cheater). The system should be able to identify cheaters and minimize their possibilities to gain a high ranking. On the other hand, fair players should be able to gain high ranking depending on their skills and experience. In general, players should be motivated to avoid cheating as counterproductive: after some time both the reputation and rankings of cheaters should be lower than those of non-cheaters.

We adopt in particular an interdisciplinary approach in this paper that mixes computing technical knowledge and competences with social sciences empirical research. In-

deed, we are convinced that building sustainable solutions for end users and service providers can be done successfully on the basis of a mutual collaboration among disciplines and by a technical design that must be informed by contextual and situational knowledge of social needs (i.e. we reject the ideas of social models and user requirements that can be just transplanted/implemented into technical solutions). In particular, we are guided by a critically informed approach to top-down design models and we argue for end user engaged approaches which can take into account contextual information and technical limitations.

The remainder of this paper is organized as follows. In section 2, we discuss the issue of cheating in online games in the context of existing work. Our approach is described in the following three sections. Firstly, section 3 introduces the main concepts related to player status, ranking and reputation. Section 4 then provides an empirically informed architecture for managing trust and consequently reputation and section 5 presents a formalized model for integrating ranking and reputation. Simulations of various scenarios involving sequences of encounters between players, with an initial implementation of our reputation and ranking model in place, are described in section 6. Finally, section 7 contains a discussion of conclusions and scope for further work.

2. CHEATING IN ONLINE GAMES

Cheating is common in multiplayer games but is difficult to prove [7]. Clearly the Internet provides players with a variety of opportunities and methodologies necessary to cheat in online games, in a situation in which anonymity and easy exchange of cheating techniques (i.e. cheating tools such as bots, macros or multi-clienting software) play a major role.

What is defined as cheating in digital games is often a matter of debate that involves several actors and technologies, including players, service providers, governance documents (such as End User License Agreements and Terms of Service) and anti-cheating solutions. Indeed, to break the game rules or exploit the game mechanics and obtain unfair advantage cannot always be easily defined. In many cases it is hard to precisely define the area and draw a line between cheating and not-cheating. Some players or even game providers might find the practice of writing simple macros to carry out repetitive tasks acceptable, whereas others might consider this a form of cheating. Again, some players might find the use of walkthroughs acceptable whereas other may consider this a form of cheating.

In this regard Consalvo [8] has noticed that often what is at the centre of these negotiations are what she calls "soft rules", or in other worlds those game rules that do not directly depend on the game computer code and that "can be broken more easily than the game code" ([8], p.87). Consalvo, seems to argue that these "soft rules" are more or less social rules and norms that can be found in virtual worlds. This exploitation of "soft rules" might happen for example in trade exchanges or in other cooperative actions among players. Therefore, while we can agree that cheating gives unfair advantages to players, we also must recognize the socially negotiated process that leads to something being defined as cheating. Despite this uncertainty in defining cheating, a number of different practices are commonly identified as such, including lagging, user settings, exploits, ghosting, aimbotting and triggerbot, wallhacking, disconnecting, custom kicking, stacking, farming, etc. (for a comprehensive

typology of cheating in online games, see [9] and [10]).

The multi-faceted nature of cheating in online games makes cheating detection and prevention very difficult. Nonetheless, several efforts have been made to address this problem. Some examples of anti-cheating techniques that can be found in academic literature include the use of CAPTCHAs to detect 'bot' users [11], anti-cheating protocols [12], techniques for preventing software client modifications [13], and techniques used to detect cheats in real-time games [14]. Game developers and third party software developers have created or are developing technologies that attempt to prevent cheating. Anti-cheating tools are commonly used in popular games such as *WoW*. A few examples of game specific anti-cheat tools software are *DMW Anticheat*, *GameGuard*, *PunkBuster*, *VAC*, *ProtectEnviron* or the *Warden*. Consalvo ([8], ch.6) for example identifies and describes three different typologies of tools: (1) tools that seek to prevent cheating (for example by encrypting communications between server and clients), (2) tools that seek to render cheating ineffective (for example by disconnecting the cheater once detected), and finally (3) tools that seek to detect the use of third party software (such as bots) that tamper with software clients and that, allow game companies to detect and ban cheaters.

One of the central concerns that relates to cheating is why people do it: the motivations behind cheating. Our goal here is not to exhaustively address this problem but rather to highlight the social dimension of the problem. For example, according to Parker [15], a "cheater cheats in order to have a better chance of achieving their goals whatever they are" (p.2). Hoglund and McGraw [16] for example clearly identify that one of the main reasons for cheating is obtaining revenues (i.e. real money), where there are individuals who make thousands of dollars by for example exploiting bugs and duping items, that are successively sold in exchange of real money. So, Hoglund and McGraw even come to suggest that "cheats come closest to actual crime when they are used to make a great deal of money" (p.8). Other motivations for cheating are listed by Consalvo ([8], p.95) who identifies the boredom of some of the game tasks, the difficulty of the game, the limited scenarios or even just bad games. For Hoglund and McGraw another reason for cheating in MMOGS is to level up quickly or to acquire rare items. Finally Consalvo even identifies that some players just cheat for the pleasure of doing it.

3. OUR APPROACH

Our approach is based on the integration of ranking and reputation mechanisms. In order to identify cheaters with high probability, we will base our reputation system on accusations of cheating made by players. We argue that, if the proportion of cheaters is smaller than the proportion of non-cheaters, then the non-cheaters can actively reduce both the ranking and reputation of those avatars belonging to cheaters and, as a result, diminish the motivation for cheating. Such a virtual social system will be transparent and can be supported by a properly designed Cheating Prevention System (CPS).

3.1 Cheating Prevention System

How should the cheating prevention system behave? By understanding this, we can then properly integrate the reputation and ranking systems. The following could be considered as requirements of such a CPS:

- There should be no cheaters among top ranking avatars;

- Avatars of suspected regular cheaters should have in general lower reputation than non-cheaters;

- Some non-cheaters should be able to gain higher ranking than suspected regular cheaters;

- The system should be fair with respect to all non-cheaters: avatars with better skills and experience should have higher ranking.

The CPS should be able to identify cheaters and minimize their chances of gaining a high ranking. On the other hand, fair players should be able to gain high ranking depending on their skills and experience.

In general we would like that players with low reputation should not have high ranking or have the possibility to gain it easily. Players with high reputation should be able to gain high ranking according to their skills and experience.

3.2 Introduction to Game Rankings

In MMOGs, ranking can be defined as a progressive structure/level of game avatars that might include several dimensions. The ranking of avatars is constructed in a number of ways. In games like *WoW* or *Tibia*, (see figure 1) for instance, this is handled through a system of linear, progressive empowerment measured by 'experience'. As an avatar explores, kills Non Player Character (NPC) monsters, and completes quests, they will accrue experience, which in turn increases their level. Progressive levels represent greater competency of the avatar, measured through character attributes such as 'intelligence', 'strength', and so on. Gaining levels in turn allows the user to tackle more difficult quests and monsters. This system ranks avatars, and is primarily a function of time. Experience may be gained from certain forms of player-versus-player (PvP) combat in WoW, but the reverse of this does not hold true; it is impossible for one avatar to reduce the experience points of another through combat. In Tibia instead the level of an avatar can decrease when the avatar is killed either by monsters or by other characters. This is called the 'death penalty' and varies also according to the overall ranking of an avatar.

The use of levels is the most popular means by which avatars in MMOGs are ranked, but there are other systems. *EVE Online*, for example, uses 'skills' to represent more specific abilities and traits an avatar embodies. Rather than utilize quests or monsters, an avatar in *EVE Online* learns skills automatically, requiring nothing more than time. To an extent in *EVE Online*, 'age' replaces 'level' as a metric for judging the ranking of an avatar, and an avatar with more skills will generally be more capable than an avatar with fewer ones.

The systems described above both introspectively gauge the avatar against the system they inhabit in that they rank 'time', rather than 'ability' or 'knowledge' which would serve to measure the user rather than the avatar. However, other examples of ranking can be found within *WoW*, through its *Arena* and *Battleground* competitions. For example, ranking within *Battleground* is fleeting; the data posted to the scoreboard lasts only as long as the match itself.

3.3 The Concept of Reputation

Reputation is what is generally said or believed about a person's or thing's character or standing [17]. In partic-

Ranking for Experience on Berylia

World Selection

World: Berylia [Submit]

Rank 26-50

Rank	Name	Level	Points
1	Szuszkin	289	396887792
2	Lord Executer	281	364139470
3	Amorozo the Knight	271	324442321
4	Byna	260	287638824
5	Boroth Flam	248	248367275
6	Ziitoz	245	239905343
7	Sir chema	242	233189515
8	Komanndoos	238	221185520
9	Wiglaseek	235	212266694
10	Xaharde	231	201007789
11	Dratwik	229	196370141

Figure 1: Ranking Table of a *Tibia* server (with the 11 highest ranked characters according to level)

ular, reputation can be considered as a collective measure of trustworthiness based on the ratings from members in a community [17]. Reputation is known to be a ubiquitous, spontaneous and highly efficient mechanism of social control in societies and perhaps this is the reason why it is used as a mechanism to stabilize social relationships in computer-meditated communications, including therefore in virtual societies such as online games. The central feature of reputation is clearly described by [18] as follows "We wish to know the sort of person we are dealing with before we deal with him" (pg. 54). In other words, we would like to know the qualities of other people when we interact with them and we also wish to know how they are judged by the social groups to which we belong.

Prior to the advent of the Internet, reputation was assessed mostly via personal and face-to-face interactions. Vendors provided references, offices tallied complaints, and past personal experience and person-to-person gossip told you on whom you could rely and on whom you could not [19]. With the advent of the Internet, assessment of reputation is implemented in technological systems that can be used for enhancing online reputation. Some of these systems are well known, such as *eBay*'s rating system or *Slashdot*'s *karma*. Systems like this simply assign a numeric value to the past behavior of actors and compute a general value of reputation (i.e. the sum of all the feedback of people who have dealt with the actor). For a review, see [17].

Trust and reputation relationships exist also in MMOGs (e.g. [4, 20]). According to Taylor [4], in MMOGs we find complicated systems of trust, reliance and reputation that often find major expression in the relationships among guilds' members, or even in other types of relationships such as trade and exchanges. There are currently some reputation systems in MMOGs, but they have disparate goals and none of them specifically intervene in rankings and against cheating [21].

As noted in [22] an independent flexible reputation system (or service) is required for many MMOGs. In this paper, we examine the integration of a reputation system with the

internal ranking system. This will potentially significantly improve the user experience and scalability of MMOGs.

Kaiser and Feng [23] have developed a distributed reputation system for MMOGs that allows players to be informed of previous misbehaviour by others and encourages the formation of social networks of players that exclude those with poor reputation. One general problem with reputation systems, noted by [23], is the issue of Sybil attacks [24] where a participant effectively erases a poor reputation by creating a new persona. The requirement to purchase software and pay a subscription to participate in MMOGs helps to mitigate this, though we need to be wary of new players using free short-term trial accounts. Reputation systems in other domains, such as *TrustRank* [25], encourage the formation of social networks that can reduce the effect of Sybils.

The main objective of this paper is to develop an approach that enables the management, limitation and perhaps also prevention of cheating on the basis of the reputation ratings provided by the player community. The main idea behind this approach is based on a tight integration between the ranking of players and a reputation system. In our model, players can rate/accuse each other if they suspect the other party of cheating. The motivation behind this approach is that if a player's negative reputation can negatively influence her ranking, then this should discourage cheating. Indeed we can use accusations, the results of games between players and current reputation of the players as the basis for updating the values of reputation and player ranking. As we will see later, using some updating policies for both reputation and ranking we can discourage cheaters. In this "fair" system the game producers, non-cheaters and technology should be able to combine to identify cheaters with high probability and minimize their possibilities to gain a high ranking.

4. DISTRIBUTED TRUST & REPUTATION MANAGEMENT

4.1 Representing reputation

Rather than having an entirely centralized view of reputation, our system has the ability to manage reputation in a distributed fashion. By this, we mean that the reputation of a player is an aggregation based on how much other players trust that this player is not a cheater. This has the potential to make it harder for a cheater to 'game' the reputation system, as all players will not necessarily detect possible cheating and do reputation updates in the same way. In any case, trust by its nature is subjective and thus best managed by the entity doing the trusting.

This approach is consistent with Gambetta's definition of trust as "a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, ..." [26]. In the simplest case, we model reputation/trust as being in a (0,1) range, representing a behavior probability value as outlined by Gambetta.

4.2 Trust Overlay Architecture

As in earlier work in a different context (security in peer-to-peer networks) [27], we propose the overlay of a distributed trust management infrastructure on top of the game infrastructure. With this architecture, illustrated in figure 2, a trust management overlay operates separately from all as-
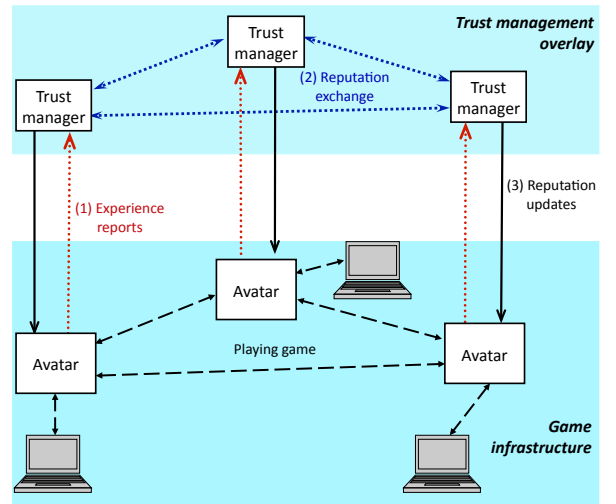

Figure 2: Trust management overlay

pects of the game. Two message passing interfaces are defined between the game layer and the trust management layer and another between the trust managers of individual nodes.

The interfaces are as follows:

(1) *Experience reports: Game engine → Trust manager*
(2) *Reputation exchange: Trust manager ↔ Trust manager*
(3) *Reputation updates: Trust manager → Game engine*

Game operation is as normal and is not directly affected by the collection and sharing of reputation information. The trust manager gathers game experience and uses this together with the experience of collaborating players to inform its trust in other players.

We then need to have a system to build trust as players gain experience of each other or learn of each other's reputation. In our system, trust can be updated in two ways:
1) Direct experience: Following an interaction between two players A and B, each player may choose to update its trust in the other based on the other player's behavior.
2) Reputation: Player A notifies selected other players of the reputation score that it has for player B. This will change significantly following an interaction where A thinks that B is cheating. How a player selects others with which to share reputation information (the player's *social network*) is significant. There is scope for further work on the formation and role of social networks in for sharing reputation information to improve cheater detection.

5. INTEGRATED REPUTATION AND RANKING MODEL

In our approach we assume that each player i has two parameters: ranking R_i and reputation/trust T_i. Both these parameters are not necessarily numbers. They can be vectors but, for the sake of simplicity in this paper, we will assume that they are just numbers. Moreover for modelling purposes we will assume that both the parameters are between 0 and 1. The top and bottom ranking correspond to 1 and 0, respectively. Similarly, the highest and lowest reputation will correspond to 1 and 0, respectively.

Game Encounter. During the online game, a player is involved in multiple interactions with other players, with some result for the player including fights with other player(s), collaboration, trading, etc. We will describe such interactions as encounters. In this paper, for modelling purposes and for the sake of simplicity, we will think of fights only but our approach is applicable to different types of encounters.

We will assume that each game encounter E between players i and j results in a value $G_{i,j} = G_{i,j}(E)$ that is equal to *Win*, *Lose*, *Draw* or *NA* depending on whether player i wins, loses, draws against player j. When the result of game encounters is not defined then we will use the *NA* result (not applicable).

Mutual Accusations of Cheating. After each game encounter E, players can accuse or not accuse each other of cheating. We introduce the *accusation function* $A_{i,j} = A_{i,j}(E)$, which is equal to *Accuse* or *NotAccuse* depending on whether player i accuses player j of cheating or not during their game encounter.

Encounter scores. After each game encounter between two players i and j, the scores $S_{i,j} = S_{i,j}(E)$ for both players are generated according to the following formula:

$$S_{i,j} = \alpha \cdot P_{\text{res}}(G_{i,j}, R_i, R_j) + \beta \cdot P_{\text{ac}}(T_i, T_j, A_{i,j}, A_{j,i}), \quad (1)$$

$$S_{j,i} = \alpha \cdot P_{\text{res}}(G_{j,i}, R_j, R_i) + \beta \cdot P_{\text{ac}}(T_j, T_i, A_{j,i}, A_{i,j}), \quad (2)$$

where $P_{\text{res}}(\cdot, \cdot, \cdot)$ and $P_{\text{ac}}(\cdot, \cdot, \cdot, \cdot)$ are policies (or policy functions) that influence the score value. In our model we will assume that $S_{i,j}$, P_{res} and P_{ac} takes values between -1 and 1. Parameters $\alpha > 0$, $\beta > 0$ are fixed and $\alpha + \beta = 1$.

We note that $P_{\text{ac}}()$ depends on the reputation of both players and mutual accusations. On the other hand, $P_{\text{res}}()$ depends on the players' rankings and the result of their encounter.

Reputation and Ranking Update Based on scores $S_{i,j}$ and $S_{j,i}$, the reputations T_i, T_j of players i, j are updated as follows:

$$T_i = \max\left(a \cdot T_i + (1 - a) \cdot P_{\text{ac}}(T_i, T_j, S_{i,j}, S_{j,i}), 0\right) \quad (3)$$

$$T_j = \max\left(a \cdot T_j + (1 - a) \cdot P_{\text{ac}}(T_j, T_i, S_{j,i}, S_{i,j}), 0\right) \quad (4)$$

where $0 < a < 1$ is a fixed parameter. On the other hand, the rankings R_i, R_j of players i, j are updated as follows:

$$R_i = b \cdot R_i + (1 - b) \cdot S_{i,j}, \quad (5)$$

$$R_j = b \cdot R_j + (1 - b) \cdot S_{j,i} \quad (6)$$

where b is some (fixed) parameter, $0 < b < 1$.

We note that the ranking update for players i, j depends on scores $S_{i,j}$, $S_{j,i}$ only while the reputation depends on P_{ac} as well as scores $S_{i,j}$, $S_{j,i}$.

Examples of Policy Functions. Here we provide some examples of policy functions that will illustrate our approach. We note that similar policy functions are used in our experiments.

The policy function $P_{\text{res}}(G_{i,j}, R_i, R_j)$ should reflect the rankings of both players. The example below gives an idea how it could look:

$$P_{\text{res}}(G_{i,j}, R_i, R_j) =$$

$$\begin{cases} A_+ \cdot R_j, & \text{if } i \text{ is a winner and } j \text{ is a loser;} \\ -A_- \cdot R_j, & \text{if } i \text{ is a loser and } j \text{ is a winner;} \end{cases} \quad (7)$$

where A_+ and A_- are some fixed parameters (e.g. $A_+ = A_- = 1$).

On the other hand, the policy function $P_{\text{ac}}(T_i, T_j, A_{i,j}, A_{j,i})$ should reflect the difference in reputations between the players and, obviously, mutual accusations. The example below gives an idea of how it could look:

$$P_{\text{ac}}(T_i, T_j, A_{i,j}, A_{j,i}) =$$

$$\begin{cases} B, & \text{if nobody accuses each other} \\ -B_-, & \text{if } i \text{ is accused by } j \text{ and } T_i < T_j \\ B_+, & \text{if } i \text{ accuses } j \text{ and } T_i > T_j \\ T_i - T_j & \text{if } i \text{ and } j \text{ accuse each other} \\ 0, & \text{otherwise;} \end{cases} \quad (8)$$

where B, B_- and B_+ are some fixed parameters (e.g. $B = B_- = B_+ = 1$).

6. PERFORMANCE EVALUATION

6.1 Simulation Setup

We suppose that there are N players, ordered in some way, e.g. $i = 1, \ldots, N$. Typically N is large, for example $N = 1000$. The ordering of players is not important. The number of players for each experiment (simulation) is different.

A game is a sequence of encounters between players. The sequence of encounters is modeled as some stochastic process. Participants for each encounter are randomly (with some probability distribution) chosen from the set of N players. After an encounter, each of the two players involved can accuse (or not accuse) each other by claiming that an opponent is a cheater (or non-cheater).

In simulations we consider two types of players: cheaters and non-cheaters. These types of players are distinguished by their behavior: how easily they could win in encounters and how often other players make accusations about them.

6.1.1 Encounter modeling

Here we consider a simplified case where the result of each encounter for each player is either winning or losing. So the result of an encounter between two players i and j is a number $G_{i,j}$ that is either *Lose* or *Win*. If $G_{i,j} = Win$ then this means that player i beats player j; if $G_{i,j} = Lose$ then this means that player j beats player i.

We model result $G_{i,j}$ of each encounter between players i and j as a Bernoulli random variable taking two values: *Win* with probability $\mathbf{p}_{i,j}^{\text{win}}$ and *Lose* with probability $1 - \mathbf{p}_{i,j}^{\text{win}}$.

In our experiments, probability $\mathbf{p}_{i,j}^{\text{win}}$ is defined depending on players i and j. If the first player i is a cheater and second player is a non-cheater then $\mathbf{p}_{i,j}^{\text{win}} = p_{\text{cn}}$, where in our experiments we put $p_{\text{cn}} = 0.9$, i.e. a cheater beats a non-cheater in 90% of cases. If both participants are of the same type, the probability is calculated as follows:

$$\mathbf{p}_{i,j}^{\text{win}} = \frac{R_i}{R_i + R_j}, \quad (9)$$

where R_i is the rating of player i and R_j is the rating of the second player j.

So probability $\mathbf{p}_{i,j}^{\text{win}}$ is defined as follows:

$$\mathbf{p}_{i,j}^{\text{win}} = \begin{cases} p_{\text{cn}}, & i \text{ (cheater)}, j \text{ (non-cheater)}; \\ 1 - p_{\text{cn}}, & i \text{ (a non-cheater)}, j \text{ (cheater)}; \\ \frac{R_i}{R_i + R_j}, & \text{otherwise}. \end{cases} \quad (10)$$

In our experiments, we randomly define which participant is the first player and which participant is the second player. But because of symmetric properties of formula (10) this choice does not influence the result of the encounter between players. Note that the probability of winning for the player with higher rating is higher than the probability of winning for the player with the lower rating if they are both either cheaters or non-cheaters.

6.1.2 Accusation modeling

After each encounter, each of two participants can make (or not make) an accusation about the opponent. The decision about whether player i should make an accusation about player j is made with probability $\mathbf{p}_{i,j}^{\text{acc}}$. The value of accusation A_{ij} by player i about j could be *Accuse* if i made accusation about j; otherwise it is *NotAccuse*.

Accusation probability $\mathbf{p}_{i,j}^{\text{acc}}$ is calculated depending on the pair of competitors. In our simulations, the accusations can be done by a loser only. In that case the accusation probability $\mathbf{p}_{i,j}^{\text{acc}}$ is calculated as follows:

$$\mathbf{p}_{i,j}^{\text{acc}} = \begin{cases} a_{\text{cc}}, & i \text{ (cheater)}, j \text{ (cheater)}; \\ a_{\text{nc}}, & i \text{ (non-cheater)}, j \text{ (cheater)}; \\ a_{\text{cn}}, & i \text{ (cheater)}, j \text{ (non-cheater)}; \\ a_{\text{nn}}, & i \text{ (non-cheater)}, j \text{ (non-cheater)}; \end{cases} \quad (11)$$

where typically we set the parameters as follows:

- $a_{\text{cc}} = 0.8$ (cheaters accuse each other often);
- $a_{\text{nc}} = 0.9$ (a non-cheater accuses a cheater often);
- $a_{\text{nn}} = 0.1$ (non-cheaters accuse each other rarely);
- $a_{\text{cn}} = 0.9$ (a cheater accuses a non-cheater often).

6.2 Simulation Results

In this section, we present results of some simulations that illustrate the dynamics of our anti-cheating approach.

We have two types of players: cheaters and non-cheaters. In each experiment, we fix the total number of players and designate a proportion of these to behave as cheaters. The game is then modeled as a sequence of discrete encounters between two players. The players for each encounter are chosen randomly. After an encounter, each player can accuse (or not accuse) the other player of cheating.

Two scenarios are presented for illustration purposes, each with 1000 players. In the first case 10% are cheaters and in the second case 30% are cheaters. For each of these scenarios, we would like to examine the dynamics of the reputation scores and ranking scores for the players.

Reputation values can be in the range (0,1) and are initially set to 1 (high). As cheaters are detected and accusations made about them, their reputation values are reduced. Non-cheaters can occasionally be falsely accused of cheating, which may temporarily impact on their reputations as well.

Ranking scores indicates how well the player performs in the game. Rankings, for our simulations, can be in the range (0,100) and are initially set to zero for new players. As players get better at the game, their scores rise. In the case of
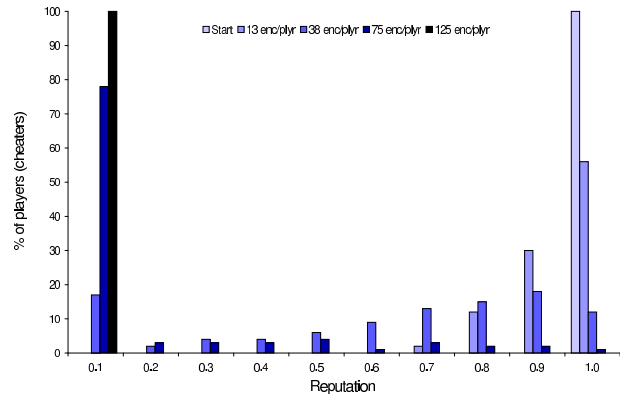

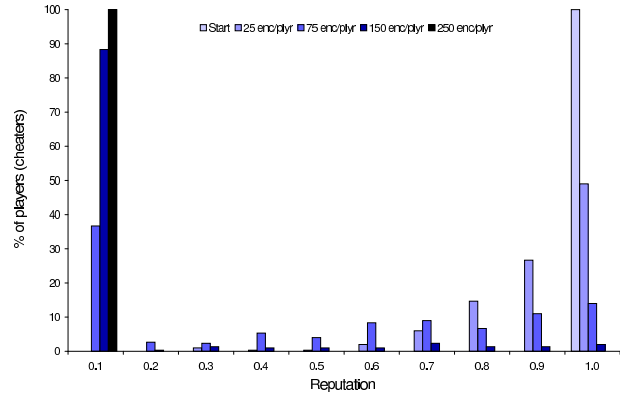**Figure 3: Cheaters' reputation statistics (10% of 1000 cheating)**

Figure 4: Cheaters' reputation statistics (30% of 1000 cheating)

cheaters, an initial rise in ranking is (hopefully) counteracted by increasing accusations of cheating and their rankings fall back towards zero. The rankings of non-cheaters can be expected to be distributed over the range of possible scores.

The histograms presented in this section show snapshots of reputation and ranking score statistics after various numbers of encounters (note that, for a large number of encounters, this number is approximately a function of time, so we are effectively seeing time dynamics). We use a roughly logarithmic scale to select the numbers of encounters after which we take snapshots for illustration. The units shown on the histograms (*enc/plyr*) denote *average number of encounters per player*. The highest value of average number of encounters per player shown in each case is chosen to be sufficient to illustrate when the system has stabilized (i.e. when all the cheaters have effectively been detected and their reputations are zero). This takes longest where the proportion of cheaters is greatest.

The histograms are scaled, i.e. the percentages of players in each range are shown, rather than the absolute number.

6.2.1 Reputation and Ranking Statistics: Cheaters

Figures 3 and 4 illustrate the dynamics of reputation for cheaters in each of the two scenarios under consideration. Initially they all have a high reputation (1.0), but accusations of cheating cause this to be reduced progressively until
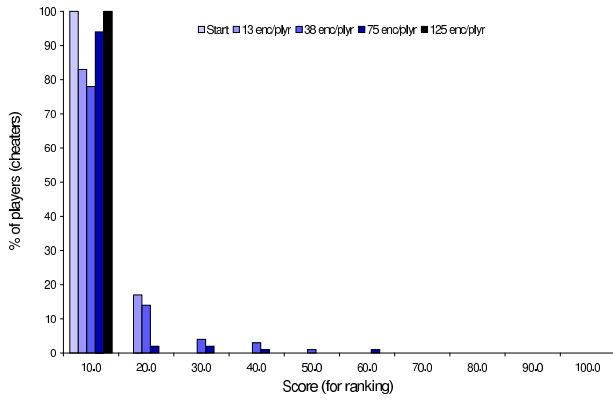
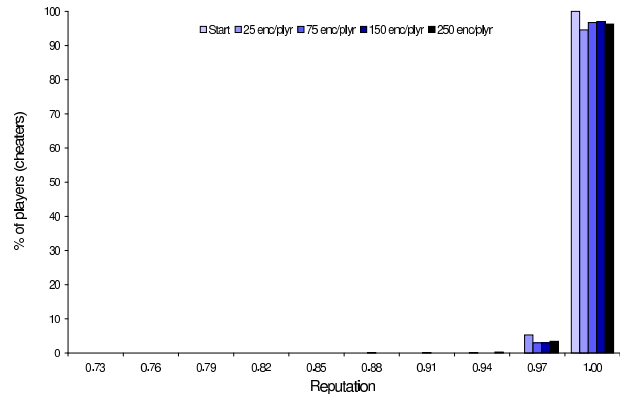**Figure 5: Cheaters' score statistics (10% of 1000 cheating)**

Figure 7: Non-cheaters' reputation statistics (30% of 1000 cheating)
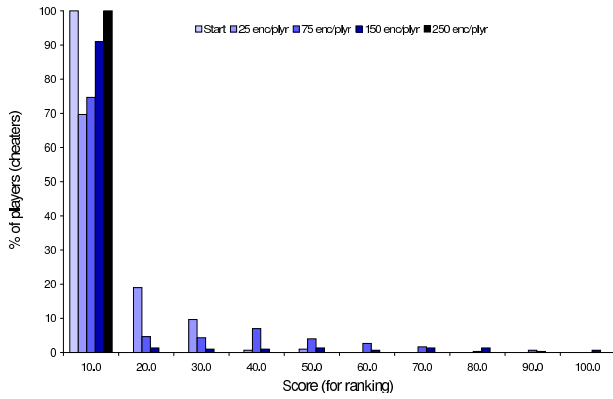

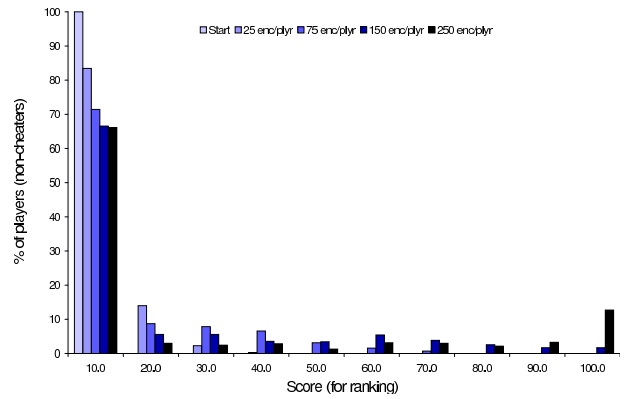**Figure 6: Cheaters' score statistics (30% of 1000 cheating)**

Figure 8: Non-cheaters' score statistics (30% of 1000 cheating)

it reaches zero. The greater the proportion of cheaters, the slower this process is.

Figures 5 and 6 illustrate the dynamics of ranking scores for cheaters in each of the two scenarios under consideration. Initially scores start at zero and then tend to rise initially. Then the rise in score is counteracted by increasing accusations of cheating and their scores fall back towards zero.

6.2.2 Reputation and Ranking Statistics: Non-cheaters

Figure 7 illustrates the dynamics of reputation for normal players (i.e. non-cheaters) in one of the scenarios, specifically the 30% cheaters case. A small number of non-cheaters can tend to fall below 1 while cheaters are still present with some reputation intact, but this is resolved as cheaters are correctly detected. Figure 8 illustrates the dynamics of ranking scores for normal players in the same scenario. Players tend to get better at the game over time.

7. DISCUSSION

We believe that the approach proposed in this paper has much potential in supporting activities such as the identification or even the prevention of cheating activities in MMOGs. In particular it is important to keep in mind that what is proposed here is a system that could help game providers to remove those cheaters that are at the top of the game rankings and that are there precisely because of cheating.

7.1 Limitations and scope for future work

It is clear that cheating is not always easy to define and it involves a range of different activities (e.g. farming, botting, manipulation of trust, bug exploits, and so on) and that perhaps the reputation/ranking system could suffer from how players and game providers define cheating. We are also aware however that many of these cheating practices cannot be easily controlled by means of purely software solutions. This is certainly the main reason why we rely on an additional "social mechanism" (reputation/ranking) to identify cheating. At the same time, we are aware that exploitation of the reputation system can lead itself to "cheating" and perhaps some "tamper-proof" strategies will be required.

7.1.1 Multiple Avatars

An approach that only trusts a single avatar has the following limitations:

- Multiple avatars can be used to discredit others regardless of whether or not they cheat.

- With multiple avatars a player could manipulate reputation for his or her own advantage.

- In cases where multiple avatars are related to one single account, some checks can be made using software.

- The system could support punishment of those cases

in which there is an abuse of the reputation system by means of multiple avatars.

- Multiple avatars reporting can influence indeed reputation and ranking (for the advantage of the player).

The reputation/reporting system should take account of these issues, in particular the problem of a player possessing multiple avatars. Adopting an "account" strategy can perhaps provide the means to tackle other problems and social conflicts such as harassment or fraud. Moreover, the reputation system could embody features to allow a user who feels they have been 'accused' unfairly to contest the accusation.

7.1.2 Guilds and Social Groups

Many MMOGs encourage players to form guilds, i.e. groups of players that share the same goals. We are aware that a co-ordination of reporting operated by a guild can influence the reputation system for its own advantage and reduce both the ranking and reputation of the target(s). At the same time it may be difficult to identify if several members of a guild are colluding against other players. This can happen when guilds have facilities outside the games (e.g. an external mailing list or forum) that can be used for the organization of coordinated ratings that could significantly influence both reputation and ranking of the target player/avatar.

7.2 Conclusion

In conclusion, we are of the opinion that in some cases reputation could be part of the overall properties of an avatar, very much like experience, skills, mana(s) and other characteristics. This might be quite effective in several situations. For instance, our empirical observations of WoW suggest that, in servers where there is a strong sense of community, reputation might become important in itself. In such contexts, abuse of the reputation system or accusation of cheating might be seen as too risky. In this case, the system could constitute a useful prevention of unacceptable behavior.

8. ACKNOWLEDGEMENTS

9. REFERENCES

[1] Bell, M.F. 2008. Toward a Definition of "Virtual Worlds". *Journal of Virtual Worlds Research*, 1(1).

[2] Schroeder R. 2008. Defining Virtual Worlds and Virtual Environments. *Journal of Virtual Worlds Research*, 1(1)

[3] Castronova E. 2005. *Synthetic Worlds: The Business and Pleasure of Gaming*. Chicago University Press.

[4] Taylor T. L. 2006. *Play Between Worlds*, MIT Press, Cambridge, MA.

[5] Achterbosch, L., Pierce, R., Simmons, G. 2007. Massively multiplayer online role-playing games: the past, present, and future. *Comput. Entertain.*, 5(4).

[6] ENISA. 2008. *Virtual Worlds, Real Money Security and Privacy in Massively-Multiplayer Online Games and Social and Corporate Virtual Worlds*.

[7] Pritchard M. 2000. *How to Hurt the Hackers: The Scoop on Internet Cheating and How You Can Combat It. Game Developers.* July, 2000.

[8] Consalvo, M. 2007. *Cheating: Gaining advantage in videogames*. MIT Press, Cambridge, MA.

[9] Yan, J. and Randell A. 2005. A Systematic Classification of Cheating in Online Games. *Proceedings of NetGames 05*, pp. 1-9, ACM, New York, Oct. 2005.

[10] Yan J.,Choi H.J. 2002. Security Issues in Online Games. *The Electronic Library*, 20(2), 125-133.

[11] Golle P. and Ducheneaut N. 2005. *Preventing bots from playing online games*. Computers in Entertainment, 3(3), 1-10.

[12] Di Chen, B., Maheswaran, M. 2004. A cheat controlled protocol for centralized online multiplayer games. In *Proceedings of NetGames 04*, pp. 139-143. ACM, New York, August 2004.

[13] Mönch, C., Grimen, G., Midtstraum, R. 2006. Protecting online games against cheating. *Proceedings of NetGames 06*. ACM, New York, October 2006.

[14] Ferretti, S., Rocetti, M., 2006. AC/DC: an algorithm for cheating detection by cheating. In *Proceedings of NOSSDAV 2006*. Newport, Rhode Island, Art. No. 23.

[15] Parker, J. R. 2007. Cheating by video game participants. In *Loading* 1(1).

[16] Hoglund, G. and McGraw, G. 2008. *Exploiting Online Games: Cheating Massively Distributed Systems*. First. Addison-Wesley Professional.

[17] Jøsang, A., Ismail, R., and Boyd, C. 2007. A survey of trust and reputation systems for online service provision. *Decis. Support Syst.* 43, 2 (Mar. 2007).

[18] Dasgupta, P., 1988. Trust as a Commodity. *Trust: Making and Breaking Cooperative Relations*. Blackwell, Oxford.

[19] Resnick, P., Kuwabara, K., Zeckhauser, R., and Friedman, E., 2000. Reputation systems. *Communications of the ACM*, 43(12), 45-48.

[20] Smith, J. H. 2003. Avatars you can trust - A survey on the issue of trust and communication in MMORPGs, in *Game Research - the art, business and science of computer games*, September 10, 2003.

[21] Tulathimutte T. 2006. Trust, Cooperation, and Reputation in Massively Multiplayer Online Games, November 2006, in *Game Research - the art, business and science of computer games*, November 16, 2006.

[22] Tang, L., Li, J., Zhou, J., Zhou, Z., Wang, H., and Li, K. 2005. *FreeRank: Implementing Independent Ranking Service for Multiplayer Online Games*. In Proceedings of NetGames '05. ACM, New York, 1-7. October 2005.

[23] Kaiser, E. and Feng, W-C. *PlayerRating: A Reputation System for Multiplayer Online Games*, in Proceedings of NetGames 2009, November 2009.

[24] Douceur, J. *The Sybil Attack* in Proc. International Workshop on Peer-to-Peer Systems. March 2002.

[25] Gyöngyi, Z., Garcia-Molina, H., and Pedersen, J. 2004. *Combating Web Spam with TrustRank*. Proceedings of VLDB, Toronto, September 2004.

[26] Gambetta, D. 1988. *Can we trust trust?* Trust: Making and Breaking Cooperative Relations. Blackwell, Oxford.

[27] McGibney J. and Botvich D. 2007. *Distributed dynamic protection of services on ad hoc and p2p networks*, Proc. 7th IEEE IPOM Workshop, San Jose, LNCS 4786 (November 2007), Springer, 95 – 106.