Cheating Resistance of P2P Gaming Overlays

Muhammad Ikram*, Kamill Panitzek†, Max Lehn‡, and Thorsten Strufe*
*Peer-to-Peer Networks, †Telecooperation Group, ‡Databases and Distributed Systems Group,
Department of Computer Science, Technische Universität Darmstadt

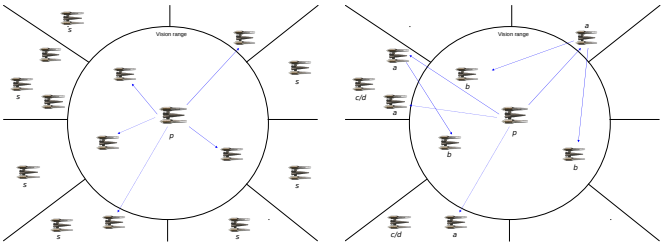
***Abstract*—P2P-based massive multi-player online games (MMOGs) use information dissemination overlays for exchanging game control and position updates among players or peers. Although these overlays are massively scalable and accommodate highly dynamic peers, yet they are prune to deliberate perturbations or cheating by adversaries. Cheating in MMOGs lead to poor quality of gaming services, unavailability of gaming services and hence dissatisfaction of players and/or losses for the companies providing these games. To solve cheating on availability and on quality of gaming service in MMOGs, we propose an indirection-based cheating resistance scheme. In our study[1], we concentrate on cheating in P2P-based first person shooter games and investigate the affect of cheating on gaming service quality and availability. We envisioned that our scheme prohibits a class of cheating in first person shooter MMOGs and maintains quality of gaming services mainly availability and responsiveness.**

I. Introduction

The development of MMOGs have shown to be quite profitable, the huge number of people playing simultaneously introduces a completely new set of problems. The main problem is the difficulty to support the game server. On one hand big server farms are needed just for the computation of the game state. This is very expensive and can be error-prone because it introduces a single point of failure. On the other hand the sheer number of people playing at the same time requires a huge amount of traffic going in and out of the server. This can also become expensive with the growth of the number of people simultaneously playing and can lead to game lag if the server can not support that many players. Game lag can be very frustrating to players and thus can lead to players dissatisfaction, resource misuses and profit losses and hence lead to gaming service's scalability problems.

To tackle the scalability problems, a P2P *gaming service overlay* can be used to discover and distribute the game service among players i.e., peers or nodes. P2P gaming service overlays are next generation P2P systems. Their requirements as well as occurring problems are described in the related work by Kamill Panitzek. The main reason to use such systems is that the maintenance of server farms that are able to provide such large scale applications is a challenging and costly task. However, using a P2P gaming service overlay as a network infrastructure can have a direct impact on the quality of experience of a game. Yet, the autonomy of control over game load and storage, lack of centralized authority, and the use of open P2P protocols results in greater security risk i.e., cheating in P2P-based gaming services. Our goal of cheating resistance is to ensure gaming services availability and high performance without affecting the scalability of the whole system.

Cheaters are the players (also called *peers* or *nodes*) who try to get unfair advantages over other players by exploiting game protocols and local game state, duping other players via false position updates, bogus achievements distributions, eavesdropping local traffics, and most importantly denial of gaming service cheating. In this paper, we concentrate on denial of gaming service cheating problems in first-person shooter games e.g., Planetπ4 [4] which uses Voronoi-based information dissemination overlays i.e., pSense [5].



(a) **(b)**

Figure 1. (a) Shows direct interaction among players. Player P disseminates messages with all neighbors and potential neighbors - the nodes within it's vision range. (b) Shows indirection mechanism to avoid ID-based cheating in games. In this mechanism, every node p relays traffic to its direct neighboring nodes via indirection nodes A.

II. Gaming Overlays

Both pSense [5] and VON [2] interpret the vision range as a radius and the area-of-interest (AOI) as a circle on the 2D plane of the virtual game world. The overlay network topology is constructed locally at each player using the AOI radius and the relative positions of surrounding players in the game world. In pSense [5], as shown in Figure I, each player knows all his neighbors in its vision range and directly communicates with them, i.e., each node or player keeps a permanent connection for (position) updates to each neighbor as long as the latter remains in the vision range or approaching its vision range. For this purpose, each node $p \in P$ keeps one sensor node $s \in S$ for each of these sectors. Each sensor nodes s calculates distances among players in the 2D plane or 3D space projected to the terrain ground plane. In addition to neighboring nodes, a node p keeps connections to a subset of sensor nodes $S_p \subseteq S$. Sensor nodes have to notify the node about other players approaching the vision range of player p. More importantly,

[1]This work has been funded by the DFG research unit 733 QuaP2P.

Table I
CLASSIFICATION OF PLAYERS IN VIRTUAL ENVIRONMENT.

	Contact not allowed	No neighbor
Contact not allowed	B (Direct neighbors)	C (Previous relay)
Contact allowed	A (Relay only)	D (All other)

the mechanism of sensor nodes prevents network partitions particularly in low density regions where players potentially have no neighbors in the vision range.

III. CHEATING RESISTANCE OF GAMING SERVICE OVERLAY

A node p keeps an outgoing *data stream* to each known neighbor in its vision range and regularly sends update messages about it's current position. Each player knows all his neighbors, potential opponents, in it's vision range. This direct communication among the players leads to vulnerabilities, mainly privacy - the protection of information from unauthorised disclosure, in gaming service overlays i.e., pSense [5]. An adversary can infer the IP-address of a potential opponent and can launch denial-of-service (DoS) attacks, also called *cheats*, on the opponent player. We assume that an adversary has external resources, both hardware and software, that are used to send enough messages to a victim to overwhelm her resources, hence making the gaming service unavailable for the victim. In addition to unavailability, such attacks lead to gameplay lags and degradation of quality of service hence player dissatisfaction and profit losses for game providers.

Tor [1] like sender and receiver anonymity are not appropriate for first-person shooter games mainly because it is not scalable and can't fulfill real-time requirements of first-person shooter games. Moreover, Tor requires global view of the network to achieve anonymity. This global view is highly unlikely to achieve in highly dynamic and latency constraint gaming services. Similarly OneSwarm [3] proposes a data sharing protocol that seeks tradeoffs between performance and privacy of data-sharing applications yet it is not appropriate for real-time application e.g., first person shooter games.

To overcome this situation and maintain adequate quality requirements of first-person shooter MMOGs, we propose an *indirection-based cheating resistant* gaming overlay as shown in Figure I (b). Instead of direct connections among players in the vision range (as shown in Figure I (a)) of player $p \in P$, the indirection scheme classifies neighboring nodes into four categories, shown in Table I, and allows communication among players via relay nodes $a \in A$ as shown in Figure I (b).

The scheme works in a decentralized fashion, where every node $p \in P$ in the virtual world represents a player who is connected with it's direct neighboring nodes $b \in B$ via relay node $a \in A$ using indirect links L. A forwarding edge from a node p to node $a \in A$ is represented with $e = (p, a) \in L$. For a given player p, Algorithm, as given in Table II selects a subset

Table II
CLASSIFICATION OF PLAYERS IN VIRTUAL ENVIRONMENT.

Input: L ∈ A;
Output: Selecting relay node, x;
while *halt==TRUE* || *player==DEAD* **do**
  Find *best* x ∈ L;
  if *x: available for relay* **then**
    use x as relay;
  end
  else
    Remove x from L;
  end
end

of indirection or relay nodes $A_p \subseteq A$. To select a relay node, node p sends multiple requests to all other potential sensor nodes to join it's *indirection tree*. Formalised as function C : S x S $\rightarrow$ {$true$, $false$} with two nodes $p, b \in P$ indirect connectivity is given if $C(p, b) = true \Leftrightarrow \exists\ x_1$, x_2, ..., $x_m \in S$, x_1 = a, ..., x_m = b, C_d (x_1 , x_2) $\wedge$ C_d (x_2, x_3) $\wedge$ ... C_d (x_{m1} , x_m) for $m \geq k$ where k is the number of indirection hops. For low latency and real-time requirements of first person shooter games, we aim for the indirect connectivity i.e., k should be small enough to guarantee real-time gaming experiences as well as large enough to eliminate the possibility of inferring IDs of possible victim nodes. Figure I (b) is a special case with k = 2.

IV. CONCLUSION

This paper presents our ongoing research on availability of P2P gaming services and cheating resistance in P2P-based first-person shooter massive multi-player online games. Once the gaming services is distributed among peers, information dissemination overlays are used to exchange game control and position information among each others. Adversaries i.e., cheaters exploit gaming services by affecting their quality of service and/or unavailability for players hence leads to dissatisfaction of players, and/or losses for the companies providing the games. Due to low-latency requirements of gaming services We are aiming at our cheating resistance mechanism to maintain real-time requirements of first-person shooter gaming services as well as to provide anonymity for the player to prevent being attacked by adversaries.

REFERENCES

[1] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: the second-generation onion router. In *Proceedings of the 13th conference on USENIX Security Symposium - Volume 13*, SSYM'04, Berkeley, CA, USA, 2004. USENIX Association.

[2] Shun-Yun Hu and Guan-Ming Liao. VON: A Scalable Peer-to-Peer Network for Virtual Environments. In *IEEE Network, vol. 20, no. 4, Jul./Aug. 2006*, pages 22–31, 2006.

[3] Tomas Isdal, Michael Piatek, Arvind Krishnamurthy, and Thomas Anderson. Privacy-preserving p2p data sharing with oneswarm. *SIGCOMM Comput. Commun. Rev.*, August 2010.

[4] Max Lehn, Christof Leng, Robert Rehner, Tonio Triebel, and Alejandro Buchmann. An online gaming testbed for peer-to-peer architectures. In *Proceedings of ACM SIGCOMMÍ1*. ACM, August 2011.

[5] Arne Schmieg, Michael Stieler, Sebastian Jeckel, Patric Kabus, Bettina Kemme, and Alejandro Buchmann. pSense - Maintaining a Dynamic Localized Peer-to-Peer Structure for Position Based Multicast in Games. In *IEEE International Conference on Peer-to-Peer Computing*, 2008.