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 prone 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, 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 game lag if the server can not support that many players. 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 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, 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.

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 1 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 to the terrain ground plane. In addition to neighboring nodes, a node p keeps connections to a subset of sensor nodes S_p ⊆ S. Sensor nodes have to notify the node about other players approaching the vision range of player p. More importantly,
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 its current position. Each player knows all his neighbors, potential opponents, in its 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.

For [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 indirect-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 indirect scheme classifies neighboring nodes into four categories, shown in Table II 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 of indirect 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 indirect tree. Formalised as function $C : S \times S \rightarrow \{true, false\}$ with two nodes $p, b \in P$ indirect connectivity is given if $C(p, b) = true \Leftrightarrow \exists x_1, x_2, ..., x_m \in S, x_1 = a, ..., x_m = b, C_d(x_1, x_2) \land C_d(x_2, x_3) \land ... \land C_d(x_m, x_m) \land \forall m \geq k$ where $k$ is the number of indirect 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 other. 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


