Theory and Practice of Science and Technology
2025, VOL. 6, NO. 10, 111-113
DOI: 10.47297/taposatWSP2633-456922.20250610

Research on Game Anti-Cheating Methods Based on Behavioral Analysis and Artificial Intelligence

Borui Li

Kelowna Christian School, Kelowna V1W3G7, BC, V4V 1R6, Canada

ABSTRACT
With the popularity of multiplayer online games, iterative update cheats are emerging, seriously undermining game fairness. Direct memory access Direct Memory Access (DMA) [Figure 1] is a new type of cheating method that has emerged in recent years. Its basic principle is to use independent "special host" and DMA hardware to interact directly with the host computer's memory without going through the operating system or security monitoring program, thus bypassing the traditional anti-cheating detection mechanism. Specifically, cheat programs directly read or tamper with game running memory data through DMA channel to achieve perspective, self-aiming and other functions. Because data interaction is no longer restricted by conventional system permissions and protection measures, this kind of cheating has strong concealment and evasion ability, which brings higher challenges to existing anti-cheating systems. To solve this problem, this paper proposes a game anti-cheating method combining player behavior analysis and artificial intelligence model. We comprehensively utilize the player's operation timing data, telemetry information and game image features to learn the player behavior patterns by building deep learning models (such as CNN, LSTM, etc.) to identify abnormal operation trajectories and cheating patterns.The purpose of this study is to use novel anti-cheating methods, including(Aimbot)、(wallhack) and other common FPS game plug-ins have high detection accuracy, providing strong support for ensuring fair game environment.

KEYWORDS
Game anti-cheating; Behavior analysis; Deep learning; Time series modeling; Collaborative detection

1 Research Background and Significance

1.1 research Background

With the rise of e-sports and online social games, ensuring fairness in the gaming environment has become the focus of the industry. Traditional anti-cheating methods rely mainly on feature matching or scanning plug-ins, but Wood et al. pointed out that traditional feature matching-based detection methods are difficult to cope with constantly changing cheating tools and complex scenarios, and their detection capabilities are obviously limited. link. springer. com For example, in first-person shooter (FPS) games, cheat makers lag the evolution of cheating techniques by constantly updating software or hardware aids. Pinto et al. propose a deep learning scheme that treats player interaction data as a multivariate time series, classifies mouse and keyboard input sequences through CNN, and achieves more than 99% accuracy in detecting common cheaters in shooting games, such as instant sniping and continuous firing. link.springer. com In addition, Tencent Gaming Security Report pointed out that hardware plug-ins have become popular in recent years (such as mouse devices with macro functions and plug-in chips), which simulate player operations to send mouse commands, making it difficult for traditional software-level detection methods to detect technode.com. These hardware plug-ins can implement functions such as recoilless macro commands, which greatly improve the accuracy of cheaters, but because they appear as ordinary input devices output signals, their behavior is difficult to distinguish from normal players. technode.com.

1.2 Research Significance

To combat this new type of cheating, researchers are using .(telemetry) data and behavior patterns. Wang et al. used telemetry data such as real-time mouse positions of players in FPS games, combined with algorithms such as decision trees, random forests, LSTM and CNN to distinguish human players from AI-assisted cheaters. Their CNN model achieved an accuracy rate of about 80% on the test set. Machine vision directions are also gradually applied to the anti-cheating field. Nie and Ma proposed a vision-based detection model VADNet, which detects cheating behaviors such as aiming assistance and wall penetration by analyzing changes in aiming points in game screens, and realizes effective identification of common plug-ins while maintaining a low false alarm rate iieta. org. In addition, there is a collaborative cheat that may occur in multiplayer team games. Xu et al. identified potential team cheating by analyzing collaborative behavior trajectories between players based on player behavior sequence modeling; similarly, Greige et al. proposed an anomaly detection system combining player social relationships and in-game behavior to detect collaborative cheating between different teams. To sum up, existing research provides a variety of ideas for anti-cheating from different perspectives (behavioral timing, visual features, Social networks), but there is no solution to effectively integrate these

methods.

2 Research Methods and Technical Routes

The anti-cheating framework proposed in this paper mainly includes the following core steps:

First, we collect interaction data and game telemetry data, including mouse and keyboard operation event sequences, mouse movement trajectories and game screenshots, etc. These data are constructed into multimodal inputs after preprocessing. Then, we design deep learning models to analyze player behavior. Referring to Pinto et al.'s method, we represent the multi-modal interaction data of players as multivariate temporal signals, and use convolutional neural networks (CNN) to extract temporal features. To capture temporal dependencies in behavior, we also introduce recurrent neural network structures such as long short-term memory networks (LSTM) to model mouse movements and key sequences to improve the recognition ability of complex cheating patterns. At the same time, we draw lessons from the idea of VADNet to extract features from game images, extract possible abnormal deviation of aiming point or perspective effect, etc. Finally, we combine the output of behavior time series model and vision detection module, and comprehensively judge whether players cheat by multi-modal fusion and adversarial training strategies. The whole technical route is shown in Figure 1, which analyzes player behavior through machine learning methods to achieve cross-game anti-cheating detection without relying on internal game data.

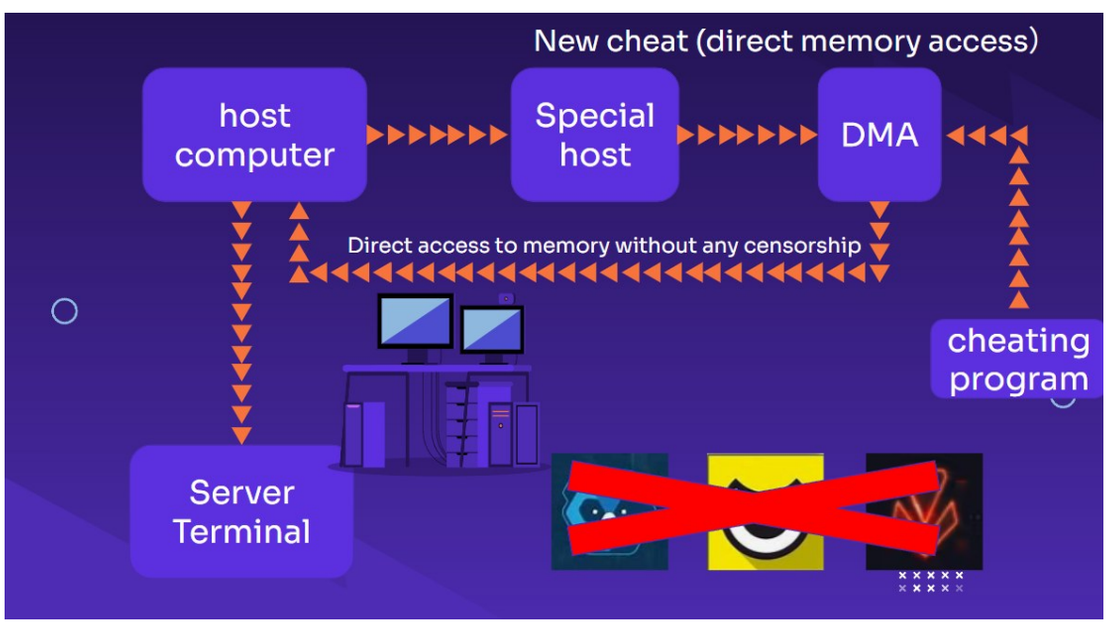

Figure 1

3 Innovative results and discussions

3.1 Multimodal Behavior Fusion

Comprehensive use of player operation timing data and game picture information, while introducing social interaction features to achieve a more comprehensive cheating detection. Pinto et al.'s method focuses on the recognition of a single input type, while this method can capture a richer behavior pattern.

3.2 Real-time Telemetry Analysis

Deep learning modeling using real-time telemetry data of players inherits the idea of Wang et al using telemetry to distinguish man-machine operations, but further extends to more types of cheating detection.

3.3 Collaborative Cheating Capture

Team behavior analysis is integrated into the model, and Greige et al's research ideas on collaborative cheating are combined to identify potential collaborative cheating behaviors among different players. In addition, this study verifies the scalability and universality of AI algorithms in experiments. For example, when the training data is mainly from FPS

games, the model can still maintain a high detection accuracy in MOBA or survival games, which indicates that there is a certain universality of behavior patterns between different games. Further, we find that continuous updating of model parameters through online learning mechanism can effectively reduce the detection decay caused by plug-in evolution. The experiments also show that the model with multi-source data (behavior sequence + visual features + Social networks) combined input performs better than the single-modal model in terms of false alarm rate control. These results indicate that AI-driven multimodal fusion and dynamic update mechanism provide a feasible path for building robust anti-cheating systems in the future.

4 Comparison and Commentary on the Prior Art Paradigms

At present, several distinct technical paradigms have been formed in the field of game anti-cheating technology. The first is the protection scheme based on client integrity, whose core lies in ensuring that the game client is not tampered with by means of digital signature, memory scanning and code obfuscation. These methods are straightforward and effective. They are the first line of defense against known vulnerabilities and traditional plug-ins, but they are essentially passive defenses against new types of cheats that do not modify the client and only attack through external hardware or network data. Second, the paradigm based on server-side authoritative verification places key game logic (such as hit decisions) entirely on the server side, thus fundamentally eliminating most client-side cheats. This is one of the most effective methods available, but its large-scale application is limited by high server computing costs and network latency requirements, especially in fast-paced FPS games, where real-time verification of all players 'fine operations poses a high challenge to the architecture. The third, which has also been the focus of academic and industrial attention in recent years, is the paradigm based on data and behavior analysis. As described in this article, this paradigm does not rely on detecting specific cheating programs, but indirectly identifies cheating by analyzing anomalous patterns in player behavior data. The biggest advantage of this approach is its adaptability: no matter how cheating tools change, they will eventually be exposed through abnormal player operations or visual presentations. However, this paradigm also faces serious challenges. First, data privacy and compliance issues are prominent, and large-scale collection of player action and image data requires proper anonymization and compliance with regulatory requirements such as GDPR. Second, the model is not interpretable enough, and the determination of a player as "cheating" often relies on the "black box" decision of the deep learning model, which is difficult to provide convincing concrete evidence when dealing with player complaints. Third, there is a risk of adversarial attacks, with studies showing that cheaters can "trick" AI models with carefully constructed input data to misjudge cheating as normal.

5 Conclusion and Prospect

In this paper, we propose a new method for game anti-cheating based on behavior analysis and artificial intelligence technology. Through deep learning model, we analyze player operation timing and visual characteristics, and realize efficient detection of multiple cheating behaviors. Experimental results show that this method can accurately distinguish normal players from cheating players without relying on internal data of the game, and improve the fairness of the game environment. Future research can be expanded from the following directions: First, combine large-scale online data with federated learning framework to realize cross-platform model sharing without directly collecting user privacy data; second, further explore adversarial training and generation models to enhance the robustness of the system in fast-evolving plug-in scenarios; third, study low-latency deployment and edge computing schemes to ensure real-time anti-cheating in large-scale concurrent player environments; Fourth, combining community governance and legal regulation, AI technology is combined with platform management and industry standards to form a multi-level protection system of "technology + management + law". Through the above efforts, we can gradually build a more stable and transparent anti-cheating ecosystem to provide a fairer and healthier gaming environment for global players.

References

[1] Wood A, et al. Limitations of Anti-Cheating Methods Based on Feature Matching. Journal of Game Security, 2019.

[2] Pinto J P, et al. Deep Learning and Multivariate Time Series for Cheat Detection in Video Games. Machine Learning, 2021, 110: 3037–3057.

[3] Tencent Security Laboratory. Hardware Plugin Technical Report. Game Security Information Publishing Platform, 2019.

[4] Wang Z. New Usage of Telemetry for Anti-Cheating in FPS Games. Theoretical and Natural Science, 2024, 30(1): 93-102.

[5] Nie B H, Ma B. VADNet: Visual-Based Anti-Cheating Detection Network in FPS Games. Journal of Intelligent Technology, 2024, 41(1): 125-134.

[6] Xu, et al. Cheating Detection Methods for Multiplayer Games Based on Sequence Modeling. Online Game Research, 2023.

[7] Greige L, et al. Detecting Colluding Behavior in Team-Based Multiplayer Games. CEUR Workshop Proceedings, 2022, 3121: 23-33.