

P2P 対戦型オンラインゲームにおける不正抑制手法の提案

伊藤 晋[†] 十川 基[†] 斉藤 裕樹[‡] 戸辺 義人[‡]

[†]東京電機大学大学院 工学研究科 情報メディア学専攻

[‡]東京電機大学 工学部 情報メディア学科

{itsin, hajime, hsaito, yoshito}@unl.im.dendai.ac.jp

1. はじめに

ネットワークゲームにおいて特定のサーバを用いず、クライアント間で直接接続しゲームを行う P2P 対戦型オンラインゲームが普及し始めている。しかし、P2P 対戦型オンラインゲームではプレイヤーキャラクタ情報の処理をプレイヤー自身のノードに行わせるため、プレイヤーによるデータの改竄のような不正行為が行われやすいという問題が存在する。そこで我々は P2P 対戦型オンラインゲームにおいて、プレイヤー情報の処理を自身で行わず対戦相手に行わせることで不正を抑制するシステム PHAM (Process Handover to Adversary on P2P Multiplayer Online Games) を提案する。PHAM を用いることで不正を自動的に検知し、不正者の抑制が容易となる。

2. P2P 対戦型オンラインゲーム

本研究において対象とする P2P 対戦型オンラインゲームについての定義を以下に示す。

- ゲームのプレイヤーは数人から十数人程でグループを作り、一時的に作られた一つのゲーム空間を共有し、その空間内でゲームをプレイする。
- 対戦相手の募集、マッチング及びゲーム戦績の記録等にはサーバを用い、ゲームプレイの際には P2P を用いる Hybrid - P2P 型の構造をとる。
- ゲームをプレイする際には、全てのプレイヤーは他の全ての対戦相手と直接接続し、プレイヤー間のネットワーク形態はメッシュ型の構造をとる。
- プレイヤーが入力した操作や対戦相手からの干渉などのプレイヤーキャラクタの状態変更情報は、プレイヤー自身のノードで処理を行い、処理結果を全ての対戦相手に送信する。

3. 目的

従来の P2P 対戦型オンラインゲームでは、プレイヤー情報を自身のノードで処理を行っているため、クライアントのプログラムやパケットを不正に改竄することで他のプレイヤーよりも優位に立つといった不正行為が行われやすいという問題が存在する。そこ

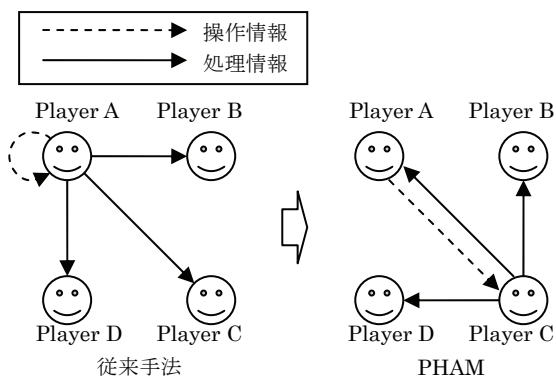


図1：従来手法と PHAM の情報配送方法例

で我々は、自分の情報処理を自身のノードで行うのではなく、対戦相手のノードに行わせることで、自身の情報の改竄を防ぎ、不正を抑制するシステム PHAM を提案する。また、対戦相手に処理を行わせることによる問題点及び解決法についても述べる。

4. PHAM 概要

本章では PHAM における不正抑制手法についての詳細を述べる。

4.1. キャラクタ処理の委譲

ゲームを始める前に、サーバはそれぞれのプレイヤーの処理ノード(PN)をグループの中から決定する。プレイヤーは必ず他の対戦相手一人の処理を担当し、互いに処理は行わないように組み合わせを行う。プレイヤーは自身の PN へキャラクタの操作情報を送信し、操作情報を受け取ったPNは操作情報を処理し、対戦相手全てにその結果を送信する。図1に4人でのゲーム対戦時における従来手法と PHAM の情報配送方法の例を示す。

4.2. 処理委譲における問題の解決

自身ではなく対戦相手プレイヤーのノードに処理を行わせることで、自身のキャラクタ情報の不正操作を防ぐことが可能となる。しかし、対戦相手の情報を処理するため、対戦相手の情報の不正操作が行われ、そのプレイヤーを不利に陥れる可能性がある。そのため、PN を監視する処理監視ノード(PMNM)を用意する。PMNM は PN と同様の方法で決定されるが、1プレイヤーのPNとPMNMが同一のプレイヤーでは意味がないためPNとPMNMを同一の対戦相手プレイヤーにしないよう決定する。表1に4人でのゲーム対戦時におけるPNとPMNMの担当の振り分け例を示す。PMNMはPNを監視し、PNの不正を検知する。次節で具体

Cheat Braking Technique for P2P Multiplayer Online Games

[†] Shin Ito

[†] Hajime Sogawa

[‡] Hiroki Saito

[‡] Yoshito Tobe

Dep. Of Info. and Media engineering. Tokyo Denki University ([†])

Dep. Of Info. Systems and Multimedia Design. Tokyo Denki University ([‡])

表 1 : 4 人対戦時の担当振り分け例

プレイヤー	処理ノード	処理監視ノード
A	D	B
B	A	C
C	B	D
D	C	A

的な PN の不正検出方法について述べる。

4.3. PN の不正検出

プレイヤーは PN と PMN の双方に自身の操作情報を送信する。例として、前進をする行動情報を送信した際に PN からその行動情報に対して後進をする処理情報が返ってきたとする。通常ではそのような想定していない処理情報が返ってくることはないため、PN で不正が行われているかもしれないと判断する。操作情報と PN から受信する処理情報の比較には操作情報と処理情報の整合を行う必要があるため、操作情報のタイムスタンプをとり、処理情報には処理を行った操作情報のタイムスタンプを付与し返信を行う。その後、プレイヤーはサーバへ PN の暫定不正通知メッセージを送信し、さらに PN から自身が送信した操作情報の処理情報の結果を尋ねるため PMN へ処理確認メッセージを操作情報のタイムスタンプを付与し送信する。処理確認メッセージを受信した PMN はタイムスタンプを基に受信した処理情報を確認し、プレイヤーと同様に想定されるものでない場合にはサーバへ PN の不正通知メッセージを送信する。想定される情報が正しく届いていた場合には、PMN はサーバへ非不正メッセージを送信し不正確認処理を終了する。

4.4. PN 以外における不正行為

不正をする PN はプレイヤーでもあり、また PMN でもある。そのため、PN における処理以外での不正行為への対応をする必要がある。

4.4.1. プレイヤーにおける不正行為

プレイヤーが行う不正として PN を故意に不正ノードとしてサーバに暫定不正通知メッセージを送信する可能性が考えられる。この場合 PMN が不正通知メッセージを送ることはないため、プレイヤーからの単独の暫定不正通知メッセージはプレイヤーが不正を行っているとは判断可能である。

4.4.2. PMN における不正行為

PMN の不正として、プレイヤーの不正と同様に故意にサーバへ不正通知メッセージを送信する可能性がある。これも、プレイヤーが暫定不正通知メッセージを送ることはないため、PMN が不正を行っているとは判断可能である。また、別の可能性として受信した処理確認メッセージに対して常にサーバへ非不正メッセージを送信する可能性も考えられる。その場合 PN が実際に不正を行っていたとしてもサーバへは暫定不正通知メッセージだけが送信されてしまうことになる。そのため、プレイヤー単独の暫定不正通知

メッセージはプレイヤーか PMN のどちらかが不正を行っているとは判断しなくてはならない。

4.5. 不正行為の再検出

不正通知および不正な不正通知はいずれにしても不正が起きなければ送信されることはないため、不正通知を受信した際にはその試合で不正が起きたと判断可能である。そのため、サーバは不正通知メッセージまたは暫定不正通知メッセージが送られてきた場合、そのゲームに参加していたプレイヤーのリストをログとして保存する。そして、管理者側でログを調査し検出数の多いプレイヤー達の監視調査を改めて行う。そのプレイヤーが不正をしていることを確認次第そのプレイヤーのゲームへの参加を拒否することで不正の排除を行う。従来の P2P 対戦型オンラインゲームではプレイヤーの不正通知はプレイヤーが手動で行うのが一般的であるため、自動的な不正検知を行うことで従来よりも素早い不正者の規制が可能であると考えられる。

5. 関連研究

GauthierDickey ら¹⁾は P2P 対戦型オンラインゲームにおいて、多数決投票でのゲーム情報更新やメッセージの暗号化を用いてパケット改竄等のプロトコルレベルでの不正行為を防止する手法について述べている。しかし、クライアント改竄のようなアプリケーションレベルでの不正行為については考慮していないため、本研究の手法と組み合わせることでより不正への対策を強固にすることが可能になると思われる。

6. 今後の課題

PHAM はプレイヤー、PN、PMN の 3 種類で構成されるため、PHAM を適用するには最低でも 3 人のプレイヤーが必要となり、2 人での対戦の場合には PHAM を適用することができない問題が存在する。そのため、現在ではゲームをプレイする同じグループ内で PN や PMN を選出しているが、グループ外のプレイヤーから選出することも考慮する必要がある。

7. まとめ

本研究では、P2P 対戦型オンラインゲームにおいてキャラクタ情報の処理を自身で行わせず対戦相手に行わせることでキャラクタ情報の改竄を防ぎ不正を抑制するシステム PHAM を提案した。対戦相手の情報を扱うことにより対戦相手の情報を改竄する可能性が発生するが、改竄が行われた場合にでも自動的に検知することが可能であり、その情報をサーバに記録し参考にすることで従来よりも素早い不正者の排除が可能となる。今後は提案手法を P2P 対戦型オンラインゲームに実装することで評価を行っていく予定である。

参考文献

- 1) C. GauthierDickey, D. Zappala, V. Lo and J. Marr: Low latency and cheat-proof event ordering for peer-to-peer games. In *Proc. of the 14th International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV 2004)*, 2004.