

eSports におけるトラフィック操作による妨害行為 の可能性および内部遅延測定方法の提案

Possibility of Sabotage by Traffic Control in eSports and Proposed Method for Measuring Internal Latency

温井 直輝† 井口 信和‡§ 矢藤 邦治¶
Naoki Nukui Nobukazu Iguchi Kuniharu Yato

1. 序論

エレクトロニック・スポーツ(以下, eSports)は, 電子機器を用いて行う娯楽, 競技, スポーツ全般を指し, コンピューターゲーム, ビデオゲームを使った対戦をスポーツ競技として捉える時の名称である[1]. 近年 eSports 市場は拡大しており, これからも市場が拡大すると予想されている[2][3]. eSports 市場の拡大に伴い, 賞金がかかる eSports 大会が開催されている. eSports 大会で使用されるジャンルとして, FPS, TPS, 格闘ゲームなどが挙げられ, 高い技術力と戦略的思考が要求される. プロプレイヤーはこれを職業としている.

しかし eSports 市場の急速な拡大と高額な賞金が発生する大会は, 不正行為やサイバー攻撃のリスクを増大させている[4][5]. このことから, 選手やチームが利点を得るために不正な手段を用いる可能性がある. 具体的には, パフォーマンスを意図的に低下させる妨害行為があげられる. このような行為は試合の公平性を損ない, eSports の信頼性と評価が下がることにつながる. 特にネットワーク遅延はプレイヤーの反応時間や操作精度に影響を与える要素であり, これが故意に操作されると競技の結果に影響し, スポーツとしての公平性が損なわれる.

本研究では, eSports における妨害行為としてプレイヤーのパフォーマンス低下を狙ったネットワーク遅延付与の可能性を示すことを目的に, tc コマンドを使用したトラフィック操作による妨害行為について検証する. また, 妨害行為を検知することを目的に, 測定用パケットと XDP プログラムを使用したネットワーク遅延測定システムを提案する.

2. ネットワーク遅延が与える影響

ネットワーク遅延がゲームパフォーマンスに及ぼす影響が研究されている. Liu らの研究[6]では, ネットワーク遅延がゲームプレイのパフォーマンスに与える影響, 特に射撃精度や反応速度, そしてプレイヤーの Quality of Experience (以下, QoE) に焦点を当てて調査した. 調査には, Counter-Strike: Global Offensive (以下, CS: GO) を使用し, 25 人の CS: GO プレイヤーを対象とした. この研究では, 4 種類の異なるネットワーク遅延 (25 ミリ秒, 50 ミリ秒, 100 ミリ秒, 150 ミリ秒) を付与することでゲ

ームプレイのパフォーマンスにどのように影響を及ぼすかを調査した. 調査結果から, ネットワーク遅延が 150 ミリ秒から 25 ミリ秒に減少するにつれて, プレイヤーのパフォーマンスと QoE が向上することが明らかになった. 具体的には, 25 ミリ秒のネットワーク遅延でのプレイヤーの射撃精度は 150 ミリ秒のネットワーク遅延時と比較して約 3% 高くなり, ゲーム内スコアも約 17% 向上した. また, QoE についてもネットワーク遅延が 150 ミリ秒から 25 ミリ秒に減少することで約 25% の改善が見られた. 具体的には, 150 ミリ秒のネットワーク遅延時における QoE の評価 (0.0~5.0 で評価) が約 3.3 であったのに対し, 25 ミリ秒のネットワーク遅延時には約 4.2 に向上した.

Xu らの研究[7]では, 使用される武器によってネットワーク遅延の影響が異なることが示された. Liu らの研究と同様に CS: GO を使用し, 42 人の CS: GO プレイヤーを対象とした. そして, 2 種類の武器 (アサルトライフル, ショットガン) を使用し, 5 種類の異なるネットワーク遅延 (0 ミリ秒, 12.5 ミリ秒, 25 ミリ秒, 50 ミリ秒, 100 ミリ秒) を付与することでゲームプレイのパフォーマンスにどのように影響を及ぼすかを調査した. 調査結果からプレイヤーのパフォーマンスは, ネットワーク遅延による影響を受けることが明らかになった. 具体的には, ネットワーク遅延が 100 ミリ秒長くなると, ショットガンでは影響は小さかったが, アサルトライフルではスコアと精度がどちらも約 15% 低下した. プレイヤーの移動アクションについては, ネットワーク遅延はアサルトライフルとショットガンの両方に同様の影響を及ぼした. ネットワーク遅延が 100 ミリ秒になると, QoE の評価 (0.0~5.0 で評価) が 4.5 から 0.5 点下がり, 4.0 となり約 11% 低下した.

3. トラフィック操作による妨害行為

3.1 妨害行為

Liu と Xu の研究結果より, リアルタイム性が要求される環境では, ネットワーク遅延の増加によってプレイヤーのパフォーマンスと QoE が低下することが示された. 近年, eSports 大会での不正プログラムを使用した不正行為や DDoS 攻撃による妨害行為が問題となっている. 今後, 故意にネットワーク遅延を引き起こして相手のパフォーマンスを妨害する行為が実施される可能性がある. 特に高額賞金が発生する大会では, このような妨害行為が重大な問題となる. 本研究では tc コマンドを使用したトラフィック操作による妨害行為について検証することで, プレイヤーのパフォーマンス低下を狙ったネットワーク遅延付与の可能性を示す.

†近畿大学理工学部情報学科, Department of Information,
Faculty of Science and Engineering, Kindai University

‡近畿大学情報学部, Faculty of Informatics, Kindai
University

§近畿大学情報学研究所, Cyber Informatics Research
Institute, Kindai University

¶近畿大学情報学部学生センター, Student Center, Faculty
of Informatics, Kindai University

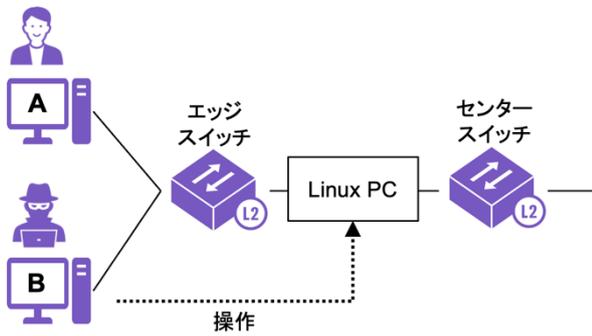


図 1 論理構成図

3.2 tc コマンド

3.2.1 概要

tc コマンド[8]は、Linux におけるトラフィック制御ツールである。このコマンドは、複数のクラスを定義し、各クラスに異なる帯域幅を割り当てることによって、トラフィック制御を実現する。例えば、重要なトラフィックに高い帯域幅を割り当てることで、アプリケーションのパフォーマンスを保証することや、一般的なデータ転送には低い帯域幅を割り当てるのが可能である。また、ネットワーク遅延やパケット損失を発生させる機能も提供し、異なるネットワーク環境下でのアプリケーションの挙動を評価することが可能である。

3.2.2 使用例

以下のコマンドは、tc コマンドを使用し特定のトラフィックにネットワーク遅延を付与するための設定である。この例では、送信元 IP アドレスが“192.168.1.1”，送信元ポート番号が“12345”，宛先 IP アドレスが“192.168.2.1”，宛先ポート番号が“80”，L4 プロトコルが“UDP”のトラフィックに+100 ミリ秒の固定遅延を付与する。

- `tc qdisc add dev eth0 root handle 1: htb default 10`
- `tc filter add dev eth0 protocol ip parent 1:0 prio 1 u32 \`
`match ip src 192.168.1.1 match ip sport 12345 0xffff \`
`match ip dst 192.168.2.1 match ip dport 80 0xffff \`
`match ip protocol 17 0xff flowid 1:10`
- `tc qdisc add dev eth0 parent 1:10 handle 10: netem \`
`delay 100ms`

3.3 検証内容与方法

本検証では tc コマンドによってネットワーク遅延を付与する妨害行為が可能であるかを検証した。検証方法の論理構成図を図 1 に示す。ゲーム用に 2 台の Windows PC を使用し、ネットワーク遅延を付与するための機器として 1 台の Linux PC を使用した。2 台の PC をそれぞれ PC A と PC B とし、Apex Legends の「射撃訓練場」でマッチングし、パフォーマンス表示機能を使用して遅延状況を観測した。PC



図 2 eSports 施設での検証の様子

B では、PC A のトラフィックにネットワーク遅延を付与する妨害行為を実施した。まず、PC B では Linux PC に SSH 接続し、tcpdump を用いて PC A で使用されている IP アドレス、ポート番号と L4 プロトコルを取得した。次に、tc コマンドを使用してサーバから PC A へのトラフィックに+100 ミリ秒のネットワーク遅延を付与した。また、ping を使用してネットワーク遅延付与を検知することが可能であるかを検証するために、継続的に PC A と PC B でデフォルトゲートウェイに対して PsPing[9]を用いた ping でのネットワーク遅延を測定した。

今回、近畿大学の eSports 施設[10]を使用して検証した。実験の様子を図 2 に示す。右側が PC A、左側が PC B のディスプレイであり、中央に設置されている機器が Linux PC である。白色のケーブルがエッジスイッチ、緑色のケーブルがセンタースイッチにつながっている。この環境で PC B から Linux PC を通じ、PC A のトラフィックにネットワーク遅延を付与する。

3.4 検証結果と考察

本検証から得られた結果について述べる。まず PC A と PC B のネットワーク遅延付与前のパフォーマンス表示機能の画面を図 3 と図 4 に示す。次に PC A と PC B のネットワーク遅延付与後のパフォーマンス表示機能の画面を図 5 と図 6 に示す。図 3 と図 4 の「ping」項目の値は、どちらも 16 ミリ秒であった。次に図 5 と図 6 の「ping」項目の値は、図 5 では 115 ミリ秒であるのに対して、図 6 では 16 ミリ秒であった。次に、PC A と PC B の ping によるデフォルトゲートウェイまでのネットワーク遅延結果を表 1 に示す。PC A と PC B で平均的なネットワーク遅延時間に違いがなく、最大ネットワーク遅延時間も 100 ミリ秒以下であるため、+100 ミリ秒のネットワーク遅延付与を検知することができなかった。この結果より、PC A の Apex Legends のトラフィックにネットワーク遅延を付与する妨害行為が可能であることが示され、ping 測定では妨害行為の検知が不可能であることが示された。

ping 測定では ICMP パケットが使用される。そのため、IP アドレス、ポート番号と L4 プロトコルを指定してのネットワーク遅延付与を検知することは不可能である。

また、パフォーマンス表示機能を使用することでネットワーク遅延状況を把握することが可能である。しかし、パフォーマンス表示機能はゲーム独自のシステムであるため、実際の計測方法は不明であり、ゲームタイトルごとに表示方法や計測内容も異なる。加えて、遅延状況を表示するだけでなく、妨害行為を検知する機能はない。したがって、内部のネットワーク遅延状況を継続的に監視し、妨害行為を検知するシステムが必要である。

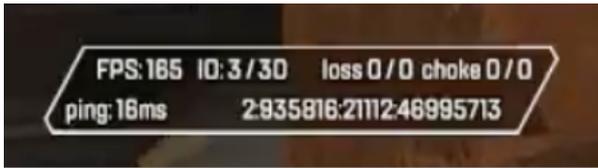


図 3 PC A 遅延付与前

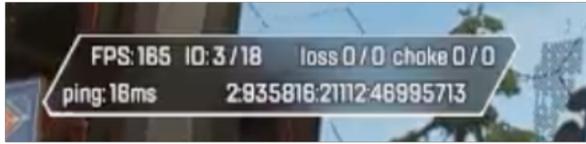


図 4 PC B 遅延付与前

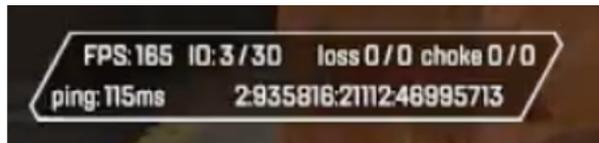


図 5 PC A 遅延付与後

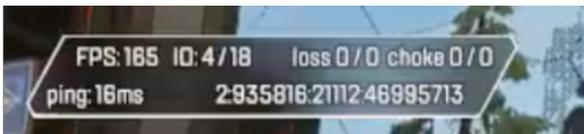


図 6 PC B 遅延付与後

表 1 Ping 測定の結果

	PC A	PC B
Sent	915	917
Received	915	917
Lost	0 (0%loss)	0 (0%loss)
Minimum	0.45 ミリ秒	0.41 ミリ秒
Maximum	32.09 ミリ秒	15.81 ミリ秒
Average	1.05 ミリ秒	0.93 ミリ秒

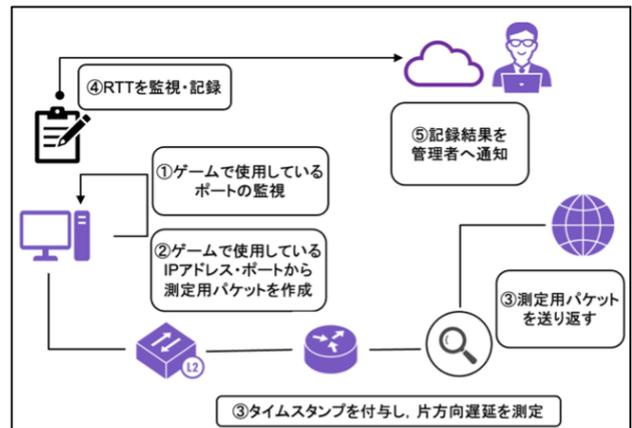


図 7 提案システムの流れ

4. 内部遅延測定システムの提案

4.1 測定用パケット

検証結果より、ping 測定では IP アドレス、ポート番号と L4 プロトコルを指定することによるネットワーク遅延付与を検知することが難しい。そこで、実際のトラフィックで使用されている IP アドレス、ポート番号と L4 プロトコルを用いた測定用パケットでのネットワーク遅延測定を提案する。これにより、ネットワーク遅延付与の妨害行為を検知することが可能である。しかし、実際のトラフィックと同様の IP アドレス、ポート番号と L4 プロトコルを使用した測定用パケットは通常のトラフィックと同様に処理される。そのため、特定の区間の Round-Trip Time (以下、RTT) を測定するために、IP ヘッダのオプション部分に「0x99」を設定する。これによりオプション部分でフィルタリングを実施し、測定用パケットである場合に特定の処理を施すことが可能となる。また、片方向ネットワーク遅延の測定を可能とすることで、ネットワーク遅延付与の検知精度を高めることが期待できる。そのため、測定用パケットには片方向ネットワーク遅延を記録するためのデータ部を挿入する。これにより、上りと下りで遅延時間が大きく異なった場合に妨害行為を疑うことが可能である。

4.2 XDP による測定用パケットの処理

測定用パケットを使用して特定の区間で RTT を測定するには、オプション部分でフィルタリングを実施し、測定用パケットを送り返す必要がある。そのため、フィルタリングに eXpress Data Path (以下、XDP) プログラムを使用する。XDP は、eBPF を使用したパケット高速処理基盤であり、

フィルタリングによるネットワーク遅延を最小限に抑えることが可能である。また、XDP プログラムで測定用パケットのデータ部にタイムスタンプを付与し、XDP_TX 機能を使用して、受信したインターフェイスから測定用パケットを送り返す。

4.3 提案システム

測定用パケットおよび XDP プログラムを使用した提案システムの流れを図 7 に示す。初めに、ゲームで使用しているポートを監視し、使用されている IP アドレス、ポート番号と L4 プロトコルを取得する。次に、取得した情報から測定用パケットを作成し、応答部分へ送信する。応答部分では、測定パケットであるかどうかのフィルタリングを行い、測定用パケットである場合はタイムスタンプを付与し、送り返す。得られる片方向ネットワーク遅延および RTT をクライアント PC にて監視し、記録する。最後に、監視結果に基づいて管理者に通知する。以上がシステム全体の流れである。このシステムを応用しアプリケーションと連携することで使用しているポート番号を動的に変更し、妨害行為からの回避・防御といった対策が可能である。

5. 今後の予定

今後は、提案するシステムにより妨害行為を検知することが可能であることを検証する。さらに提案システムが実際のゲームパフォーマンスに与える影響も調査する。また tc コマンドを使用するとネットワーク遅延付与以外にも、意図的なパケットロスやデータ部の破損、パケットの重複・順序入れ替えといった妨害行為が可能である。そのた

め、ネットワーク遅延が与える影響に加えて、それらが与える影響も調査する。

6. まとめ

本研究では、eSports におけるトラフィック操作による妨害行為について述べた。実際にLinuxのtcコマンドを使用して、特定のトラフィックにネットワーク遅延を付与する妨害行為を検証した。検証結果から、PC A の Apex Legends のトラフィックにネットワーク遅延を付与することに成功し、デフォルトゲートウェイへのping測定では妨害行為の検知が不可能であることを示した。そして、実際のトラフィックを基に作成する測定用パケットとXDPプログラムによるネットワーク遅延測定システムを提案した。

参考文献

- [1] JeSU (Japan eSports Union) : eSports とは, 入手先<https://jesu.or.jp/contents/about_esports/>(参照 2024-7-26)
- [2] FORTUNE BUSINESS INSIGHTs : eSports Market Size, Share, and Industry Analysis, By Streaming Type (Live and On-demand), By Revenue Streaming (Media Rights, Advertisement, Sponsorship, Ticket & Merchandise, Game Publisher Fees, and Others), By Gaming Genre (Real-Time Strategy Games, First Person Shooter Games, Fighting Games, Multiplayer Online Battle Arena Games, Mass Multiplayer Online Role-Playing Games, and Others), and Regional Forecast, 2024-2032, 入手先<<https://www.fortunebusinessinsights.com/esports-market-106820#:~:text=The%20esports%20market%20size%20was,share%20of%2030.34%25%20in%202022>>(参照 2024-7-26)
- [3] JeSU (Japan eSports Union) : 『日本 e スポーツ白書 2023』販売開始 豊富な情報量で国内 e スポーツ産業の市場動向を分析 2022 年の国内 e スポーツ市場は前年比 127% の 125 億円 2022 年の国内 e スポーツファンも 776 万人と増大, 入手先<<https://jesu.or.jp/contents/news/news-240131/>>(参照 2024-7-26)
- [4] WeLiveSecurity : Competing in esports: 3 things to watch out for, 入手先<<https://www.welivesecurity.com/2020/02/11/competing-esports-3-things-watch-out-for/>>(参照 2024-7-26)
- [5] TrendMicro : Cheats, Hacks, and Cyberattacks Threats to the Esports Industry in 2019 and Beyond, 入手先<<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cheats-hacks-and-cyberattacks-threats-to-the-esports-industry-in-2019-and-beyond>>(参照 2024-7-26).
- [6] Shengmei Liu, Mark Claypool, Atsuo Kuwahara, et al. : “The Effects of Network Latency on competitive First-Person Shooter Game Players”, 2021 13th International Conference on Quality of Multimedia Experience (QoMEX), 2021
- [7] Xiaokun Xu, Shengmei Liu, Mark Claypool. : “The Effects of Network Latency on Counter-strike : Global Offensive Players”, 2022 14th International Conference on Quality of Multimedia Experience (QoMEX), 2022
- [8] WIKIPEDIA The Free Encyclopedia : tc(Linux), 入手先<[https://en.wikipedia.org/wiki/Tc_\(Linux\)](https://en.wikipedia.org/wiki/Tc_(Linux))>(参照 2024-7-26)
- [9] Microsoft Learn : PsPing - Sysinternals, 入手先<<https://learn.microsoft.com/en-us/sysinternals/downloads/psping>>(参照 2024-7-26)
- [10] 近畿大学 : eSports Arena | 情報学研究所, 入手先<<https://www.kindai.ac.jp/rd/research-center/cyber-iri/esports-arena/>>(参照 2024-7-26)