Network Traffic Analysis Framework for E-Sports: The UPSIDE Dataset

Massimiliano Rak[1], Paolo Palmiero[2], and Felice Moretta[2]

Abstract With the ever-growing popularity and attendance of e-Sports competitions, the design of the network architectures which support these events has never been of such importance. Choosing the right dimensions and capabilities of networks has been more of a guessing game throughout the years, rather than a systematic approach to determining the right size, without over or under-provisioning the necessary resources. In time-limited events (physical game competitions, game events), ad-hoc network infrastructures often have technical and/or performance issues. Moreover, such temporary connections rarely integrate security countermeasures and/or are subject to security assessment. This preliminary paper aims to introduce a framework, based on real-world historical data that enables domain experts to stress test their designed networks and perform more precise and detailed capacity planning. To address this challenge, we collected and analysed real-world data from the UPSIDE event held in Naples on June 28–29, 2024. By capturing and examining all traffic on the event's network architecture, we developed a systematic framework for guiding network professionals in designing efficient and scalable infrastructures for future festivals and conventions. The data collected have been packaged in a data set that can be replicated in a modular and scalable fashion on networks to test their reliability and resiliency on different traffic scales.

1 Introduction

In recent years, the gaming industry has grown exponentially in terms of both player volume and technological complexity. According to the annual report by Newzoo,

[1]DIETI, University of Naples Federico II, Naples, Italy
e-mail: massimiliano.rak@unina.it,
[2]Department of Engineering, University of Campania Luigi Vanvitelli, Aversa, Italy
e-mail: felice.moretta@unicampania.it,
e-mail: paolo.palmiero@studenti.unicampania.it

in 2024, the gaming market surpassed $180 billion, with the number of gamers reaching 1.5 billion people. Notably, 48% of the total market, corresponding to over $90 billion, comes from mobile gaming [Newzoo, 2024]. The design and optimization of network infrastructure play a crucial role in ensuring a satisfactory gaming experience for users. The introduction of online multiplayer games, cloud gaming platforms, and virtual reality (VR) gaming solutions has significantly increased network requirements in terms of bandwidth, latency, and stability [Lyu et al., 2024].

A well-designed network ensures low latency and stable data transmission while directly influencing the *Quality of Experience* (*QoE*) for players. QoE is a multidimensional parameter encompassing gameplay fluidity, response speed to user actions, and the absence of interruptions caused by network issues. Studies show that latencies exceeding 100-150 ms significantly degrade player performance and engagement, while insufficient bandwidth can lead to packet loss and video quality drops, thereby compromising the overall experience [Flinck Lindstrom et al., 2020].

Accurate network infrastructure design is particularly crucial during gaming and e-sports events where infrastructure is tailored to meet specific needs. Such events concentrate network traffic within a defined geographic area, which can result in bottlenecks if capacity is inadequate to handle the load. A well-planned configuration is vital to ensure stable data transmission and minimal latency, contributing to a smooth and uninterrupted gaming experience.

Datasets of network traffic are indispensable for designing effective network infrastructure. They provide empirical data to understand the specific demands of modern gaming applications. By analyzing these datasets, patterns in bandwidth usage, latency sensitivity, and peak traffic loads can be identified—key factors for developing networks capable of handling high demand without compromising performance. Moreover, such insights enable the prediction and mitigation of potential bottlenecks, ensuring seamless gaming experiences [Labonne et al., 2020, Melo and de Oliveira, 2020, Namel et al., 2019].

This work, therefore, presents a dataset of network traffic collected during a competitive gaming event, aiming to provide a foundation for analyzing traffic dynamics in modern gaming ecosystems. Analyzing such data is essential to understanding the network requirements of modern games, identifying bottlenecks, and proposing targeted solutions to improve QoE. The dataset includes network traffic collected during the UPSIDE[1] gaming event, which featured several parallel sessions of various games, including MMORPGs (Massively Multiplayer Online Role-Playing Games) and FPS (First-Person Shooters) games. The game titles in question are: Clash Royale[2], EA Sports FC24[3], Brawlhalla[4], Rocket League[5], Chess[6]. While a detailed analysis has not yet been conducted, future work aims to study the traf-

[1] https://progettoupside.it

[2] https://supercell.com/en/games/clashroyale/

[3] https://www.ea.com/it-it/games/ea-sports-fc

[4] https://www.brawlhalla.com

[5] https://www.rocketleague.com/it

[6] https://www.chess.com

fic dynamics and interactions between gaming applications and network infrastructures. Furthermore, to the best of our knowledge, this research represents a novel contribution, given that our investigations have revealed the absence of publicly accessible datasets of this nature in the online domain. This dataset aims to contribute to the academic community and may provide useful insights for future research in this domain.

The rest of the paper is organized as follows: Sect. 2 reviews related work and delves into the motivations of this work; Sect. 3 describes the examined network infrastructure and the procedures and tools used to collect the presented dataset; Sect. 4 introduces the pre-processing framework for the collected data, providing a description of the various steps and tools utilized; finally, Sect. 5 discusses the results achieved so far and outlines possible future developments.

2 Related Works and Motivations

The study of network traffic in gaming and e-sports contexts has received increasing attention in recent years, driven by the rapid growth of the gaming industry and the rising complexity of networked applications. However, when focusing specifically on gaming traffic related to large-scale gaming events, a noticeable gap emerges in the availability of public datasets. This scarcity significantly hinders research and innovation in areas such as network optimization, Quality of Service (QoS) improvements, and gaming-specific infrastructure design.

Network traffic datasets are essential tools for understanding and modeling network behavior. As Melo et al. demonstrate, these datasets enable analysis of traffic patterns, bottleneck identification, and infrastructure optimization [Melo and de Oliveira, 2020]. They are also crucial for machine learning applications in traffic classification, anomaly detection, and demand prediction [Velarde-Alvarado et al., 2022, Labonne et al., 2020, Xu et al., 2020, Namel et al., 2019], ultimately improving both QoS and Quality of Experience (QoE) for users [Flinck Lindstrom et al., 2020].

A key strength of our dataset is its ability to highlight characteristics like burstiness and self-similarity in network traffic. These features are particularly important in gaming events, where traffic patterns emerge from real-time interactions between multiple players and games. According to Moon, games vary in their traffic characteristics—some show strong self-similarity and periodic packet exchanges, while others exhibit more irregular patterns. However, most games share one common trait: they exchange small-sized packets during gameplay. Our preliminary analysis confirms this characteristic in the games at the UPSIDE event, which frequently exchanged small packets with the server at high rates. [Moon, 2024, chang Feng et al., 2005, Chen et al., 2005]

Furthermore, high burstiness in traffic can significantly degrade network performance by causing congestion and increased latency, which are critical challenges in ensuring a seamless gaming experience. [Chen et al., 2005] These insights highlight

the importance of understanding burstiness to inform the design of more robust and efficient network infrastructures for gaming applications.

2.1 Limited Availability of Public Datasets

Public datasets on gaming traffic are scarce, especially those that capture data from competitive or large-scale gaming events, as evidenced by our extensive search across both search engines like Google Dataset Search and specialized platforms hosting research datasets such as IEEE DataPort. There are datasets available for general network traffic analysis. An example is the dataset *Network traffic and code for machine learning classification* [Labayen, 2020] described in [Labayen et al., 2020], which focuses on application-based traffic classification but does not encompass event-specific gaming traffic. Another example is the *ACI IoT Network Traffic Dataset 2023* [Bastian et al., 2023], which consists of real network traffic generated by a smart home, emulated in a laboratory with various IoT devices. Despite their usefulness in various contexts, these datasets lack the granularity and contextual relevance needed to understand the unique characteristics of gaming traffic. Gaming-specific datasets, when available, often focus on isolated gameplay scenarios or specific game titles, such as the *Gaming Network Traffic Dataset* [Beaini et al., 2020]. In this dataset, the authors collected network traffic generated by a PlayStation 4 over a two-week period. Data collection occurred three times daily—morning, afternoon, and evening—resulting in a total of 41 data collection rounds. Each round includes playing games like Ubisoft Club — Rogue and FIFA, along with various gaming platform interactions.

However, these datasets do not account for the highly concentrated and concurrent network usage patterns seen in gaming events, where multiple gaming sessions and genres are active simultaneously. Such complex patterns are difficult to reproduce even with the most advanced machine learning techniques, if not starting from datasets of real data. [Xu et al., 2020]

2.2 Challenges of Gaming Data Collection

One reason for the limited availability of public datasets is the difficulty in capturing and sharing gaming data, especially from gaming events. Challenges include:

- **Data Sensitivity**: Network traffic often contains sensitive information, making anonymization and public sharing complex. Additionally, this sensitivity is one of the reasons why game developers and publishers are reluctant to share server-side game data, as it may expose proprietary technologies, competitive strategies, or user-specific insights. [Moon, 2024, Xu et al., 2020]
- **Event-Specific Context**: Gaming events typically involve customized network setups, which might seem less generalizable to standard gaming scenarios.

- **Resource Requirements**: Capturing high-quality network traffic requires specialized equipment and significant coordination with event organizers and participants.

The last two points will be clearer in the following sections, where the network infrastructure of the UPSIDE event and the process of capturing network traffic will be described in detail.

Despite these challenges, gaming events present unique opportunities to study network dynamics, as they involve high traffic volumes concentrated in specific geographic areas. They also showcase diverse gaming genres, from MMORPGs to FPS, which demand varying levels of bandwidth, latency, and jitter. Moreover, the event-specific context actually represents a significant strength of our dataset, as it enables in-depth study of network traffic dynamics in these unique contexts. This, in turn, can provide critical insights to design more effective infrastructures for future gaming events, addressing challenges such as traffic bursts and bottlenecks.

3 Testing Environment and Data Collection

Understanding the complexities of gaming traffic at large-scale events requires an efficient testing environment and a well-designed data collection methodology. This section provides an overview of the infrastructure, the data collection architecture, and the types of data gathered during the UPSIDE gaming event.

The UPSIDE gaming event was a competition designed to showcase advanced gaming technologies and the capabilities of modern 5G networks. Hosted in collaboration with industry partners, including WindTre S.p.A., the event brought together competitive players and spectators in a high-demand network environment. The gaming sessions featured various popular games including Clash Royale, EA Sports FC24, Brawlhalla, Rocket League, and Chess, highlighting diverse traffic patterns and network requirements. This setting offered a valuable opportunity to study the interaction between gaming applications and network infrastructure. The private 5G network deployed for the event provided a controlled environment, ensuring data integrity and enabling precise traffic monitoring.

The testing environment was developed to capture network traffic in a real-world setting, reflecting the dynamics of gaming applications during a high-traffic, competitive event. By leveraging state-of-the-art tools and methodologies, we ensured that the captured data was representative and of high quality, suitable for subsequent analysis.

3.1 Architecture of the system under study

The network, made available by the WindTre S.p.a. partners, for the event is composed of two local networks based on 5G technology, one of them private and only

accessible from the gaming devices, for the competition's location, and an intermediate network that redirects the traffic from the latter to their data centre, which hosted a dedicated connection to the public internet, while also serving for routing the traffic to the internet for the public devices. In the data centre, other network apparatus has been dedicated to the competition such as a two set of two routers, one facing the client side of the network and the other facing the internet, and switches for reliability purposes. Both of these infrastructures can be seen in Fig. 1 and Fig. 2. For the gaming aspect, the devices used during the challenge used SIMs kindly

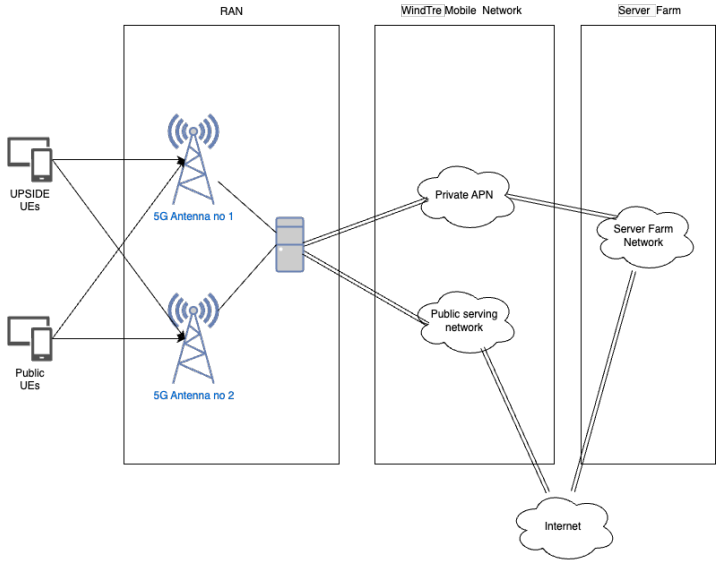

Fig. 1 Infrastructure topology of the event.

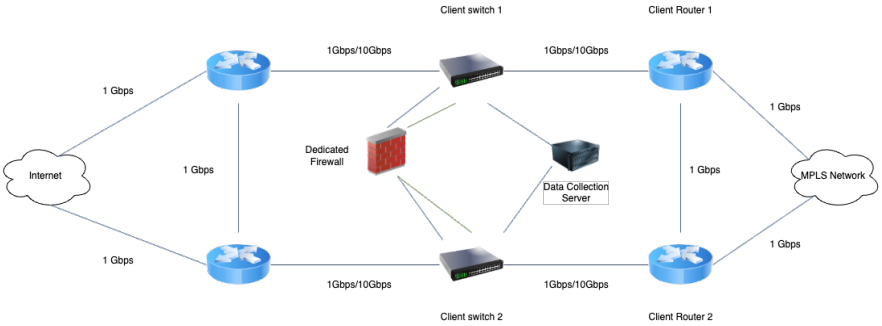

Fig. 2 Dedicated data centre infrastructure for the event.

lent from WindTre S.p.A. Each of them used a private APN, enabling them to have a private IP address belonging to the network subnet 192.168.0.1/24, routing all their traffic inside the aforementioned private 5G network.

The use of Huawei S5735-L-V2 switches played a key role in the data collection process because they integrate into their firmware capabilities for traffic mirroring, which allows them to transparently redirect all the traffic they receive to a secondary target without resorting to a "man-in-the-middle" approach that could have deteriorated the network's performance. After identifying the optimal location for placing the monitoring server, which can be seen in figure 2 and more specifically between the firewall apparatus and the client switches, the next step was selecting the most suitable software application. Following extensive research and testing, Ntopng and N2disk were chosen.

1. **Ntopng**[7] is a high-performance network traffic probe providing detailed insights thanks to its ability to gather traffic information from traffic mirrors, SNMP devices, and other systems such as IDP. It is designed for real-time analysis and offers a user-friendly interface for visualizing network activities.
2. **N2disk**[8] is a specialized application for high-speed packet capture and storage. It enables efficient network data recording to disk and supports replaying captured traffic for further analysis.

3.2 Collected Data and their data model

The data that were captured during the UPSIDE event have been thoroughly analysed for their content and we've noted that, as suggested in [Moon, 2024], the video games used during the competition exchange short but frequent packets with the various back-end services of each game. From this first result, we've been able to understand one of the requirements, thus a network designed for this e-sport tournament should emphasize more on having a low rate of packet loss rather than a large bandwidth.

The exchanged traffic is mostly made of HTTP/S requests, mostly composed of the requests necessary for web services like the retrieval of user information and/or in-game ads, and TCP communication for the actual gaming traffic generated by the game.

The rest of the packets are information exchanges between the device and the Google services, most of them using the QUIC protocol, and also other *background noise* made of DNS queries and ICMP packets.

All the recorded traffic has been divided into two different CSV files, one for the metadata associated with each packet and the other containing the Base64 encryption of each packet payload with the corresponding length.

---

[7] https://www.ntop.org/products/traffic-analysis/ntop/

[8] https://www.ntop.org/products/traffic-recording-replay/n2disk/

The metadata CSV has ten columns: *Time*, *No*, SourceIP, DestinationIP, *SourcePort*, *DestinationPort*, *SequenceNumber*, *AcknowledgementNumber*, *Protocol* and *Length*. The payload CSV has instead three columns being: *No*, *Length* and *Load*. Both the PCAP and CSV files have been anonymized accordingly for public distribution: each of all public IP addresses has been substituted with a different random IP address belonging to a different subnet (ex. *10.1.0.0/16*) depending on the game it is related to.

The full dataset is being published along with this paper and can be found at [Rak et al., 2024]. The dataset includes an Excel file containing a mapping between IP addresses and game titles, along with the features shown in Tab. 1.

No	Filename	Filetype	Total Volume (MB)	Capture Start (UTC)	Capture End (UTC)	Total Duration	Number of Packets	Number of Flows
1	28_06_1000-1330_metadata_anon.csv	Metadata	133	8:00 AM, 28/06/23	11:30 AM, 28/06/23	3.5h	1,816,723	3101
	28_06_1000-1330_payload.csv	Payload	1945					
2	28_06_1330-1830_metadata_anon.csv	Metadata	210	11:30 AM, 28/06/23	16:30 AM, 28/06/23	5h	3,121,191	4351
	28_06_1330-1830_payload.csv	Payload	1657					
3	29_06_1000-1330_metadata_anon.csv	Metadata	168	8:00 AM, 29/06/23	11:30 AM, 29/06/23	3.5h	2,484,227	3655
	29_06_1000-1330_payload.csv	Payload	879					
4	29_06_1330-1830_metadata_anon.csv	Metadata	226	11:30 AM, 29/06/23	16:30 AM, 29/06/23	5h	3,390,480	3724
	29_06_1330-1830_payload.csv	Payload	930					

Table 1 Dataset Features

No	Length	Load
1	87	FwMDAB4AAAAAAAAAsmaHqpwGatDCoJcNscYSmNmLHP7XkV4=
2	83	FwMDABoAAAAAAAAAsU9LcQpBEBomX2YUCZPkwbnQ/w==
3	91	FwMDACLjen07fw4V3ZO1ac8h/V3z6tk0RwxLhGISbEB33UMBagUH

Table 2 Example of the structure of the payload CSV.

Time	No	SrcIP	DstIP	SrcPort	DstPort	SqnceNum	AckNum	Protocol	Length
1719574200	1	192.168.0.48	10.0.0.3	54237	9339	0	0	UDP	38
1719574200	2	192.168.0.8	10.0.0.4	38926	23002	0	0	UDP	52
1719574200	3	10.0.0.4	192.168.0.8	23002	38926	0	0	UDP	52
1719574200	4	192.168.0.23	10.0.0.2	44712	443	1409452413	1977496246	TCP	101

Table 3 Example of the structure of the metadata CSV.

4 The Dataset Framework Analysis Tool

The developed framework offers a set of functionalities that aim to guide domain experts in the task of analyzing a base model traffic and subsequently aid them in designing a capable enough network. It has been written using Python as a programming language of choice, mostly for its portability and the availability of the Scapy[9] and the Pandas[10] libraries, which both made the task of analyzing data packets much simpler thanks to the range of tools that both of them make available.

These components, shown in figure 3, can be invoked individually using the command line interface or altogether ensuring a cohesive approach to data extraction, analysis and visualization. The framework is available on the VsecLab's GitHub page[11]. Following is a detailed description of the contribution each module brings.

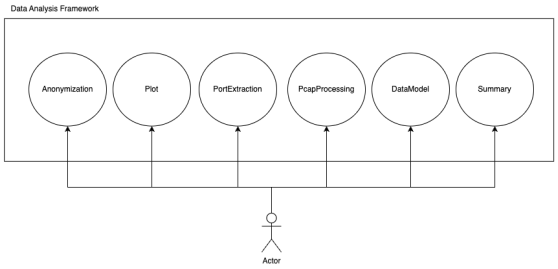

Fig. 3 Use case diagram for the framework

First, we have the **PCAP Processing** module which implements PCAP file processing functions capable of extracting all dissecting the traffic in single files for each IP belonging to an arbitrary subnet, enabling targeted analysis of traffic associated with particular network nodes. Additionally, the script supports DNS packet extraction by scanning PCAP files, identifying packets with DNS layers, and appending these packets to a new PCAP file.

For the next component, we have the **Data model** providing robust data export functions, converting PCAP data into structured CSV formats with columns such as *timestamps*, *packet numbers*, *source and destination IPs*, *source and destination ports*, *protocols*, *packets length*, and *payloads*. It includes a protocol mapping feature to identify protocols by their numbers and incorporates error-handling mechanisms to ensure resource clean-up and manage missing files effectively. Chunk-based writing further optimizes memory usage by incrementally saving processed data. This functionality is offered in three different flavours which enables the user

[9] https://scapy.net/

[10] https://pandas.pydata.org/

[11] https://github.com/VSecLab/PCAP_Analyzer.git

to choose whether to export all the network traffic information in a single CSV file, only the metadata associated or to separate the metadata and the payload of such network packets in two different files to have more flexibility during the analysis.

The information extraction from network packets has been separated further in another module to increase the flexibility of the framework.

All the collected data can then be anonymized through the **Anonymization** component to be able to share the eventually produced datasets without the need to worry about sensitive information regarding the destinations of such traffic. The *Associations* script's purpose is to identify and analyze unique associations in network traffic data, specifically focusing on combinations of source and destination IPs and ports. It reads network traffic data from a CSV file, grouping the extracted data in a tuple made of $\{$*SourceIP*, *DestinationIP*, *SourcePort*, *DestinationPort*$\}$, calculating the packet count for each unique association then sorting them in descending order based on this quantity. The output is then saved to another CSV file for further analysis or reporting. This module is particularly useful for identifying the most active communication pairs in network traffic, helping to highlight significant patterns or potential areas of interest for network security analysis or traffic optimization.

The next component is the **Plot** one, which allows to visualisation of network traffic data to uncover temporal patterns in packet transmission, focusing on specific source IPs and destination ports. The data can be read once again for a CSV file which then gets filtered on source IPs, destination ports, and a time range, all of which can be specified by the user. The examined traffic is aggregated over one-minute-long intervals: this way it can be displayed much more clearly, making this easier to understand from the human standpoint. After the filter is applied, the results are displayed in a line plot showing for each specified IP the total packet length per minute.

Then we have the **Port extraction** part of the framework that simplifies the analysis of port-based communication patterns, helping to identify commonly used or potentially suspicious ports within network datasets. This is done by extracting unique destination ports from network data to identify active or relevant communication endpoints and know applications that could be using one of the *known ports*. It isolates unique values in the *DestinationPort* column while also filtering on a given list of source IP addresses, ensuring that entries are considered only once and only for the outgoing traffic. The individuated ports are then outputted in a specific CSV file. This process becomes particularly relevant for pinpointing key ports that warrant deeper investigation, such as those that might indicate potential security vulnerabilities or require optimization in network configurations.

Last but not least there is the **Summary** component to process the network traffic data to generate a summary of the communication patterns, keeping a list of user-specified IPs in focus. It scours the traffic data filtering all the communication that has the latter IPs in the *SourceIP* and *DestinationIP*, identifying unique bidirectional sessions from which is capable of calculating the metrics such as their number, average and median duration, message counts and bit rates. The results of this computation are then presented in a summary table which aids in better under-

standing the behaviour these IPs have on the network. Following is an example of said output.

Metric	Value
Time span	5.5 h
Client-to-Server messages	165706
Server-to-Client messages	173906
Observed sessions	640
Session duration (s) (avg/med/stdev)	5010.3/845.0/6141.8
Msg per session (avg/med/stdev)	266.6/94.0/477.1
Bit rates (Kbps) (avg)	5.2
Traffic size	100.46 MB

Table 4 Example of the summary for the afternoon session during the first day of the event.

5 Conclusions and Future Works

In this work, we presented a comprehensive framework for analyzing network traffic data from gaming events. Our framework provides robust tools that enable researchers and network administrators to process, analyze, and visualize complex network interactions in gaming environments. Through modules for PCAP processing, data modeling, anonymization, and visualization, we offer a systematic approach to understanding gaming network traffic patterns.

The framework's key contributions include its modular and extensible architecture, tools for preserving analytical value while anonymizing sensitive network information, visualization features for identifying temporal patterns, and statistical analysis functions for examining communication patterns and session characteristics.

Future work could focus on several promising directions. First, the framework could be enhanced with machine learning capabilities to automatically detect anomalies in gaming traffic patterns. Additionally, we aim to develop a predictive machine learning model that can forecast network traffic requirements for gaming events based on input parameters such as the types of games to be played and expected number of users. This would enable more efficient infrastructure dimensioning and resource allocation for gaming events.

Other potential developments include the integration of real-time processing capabilities to enable live monitoring and analysis during gaming events, and the extension of the framework to support comparative analysis across different gaming events and platforms, providing insights into how network requirements vary across different gaming scenarios.

The developed framework represents a significant step forward in understanding and analyzing gaming network traffic, providing valuable tools for both research and practical applications in network management and optimization. The planned addi-

tion of predictive modeling capabilities will further enhance its utility in practical deployment scenarios.

Acknowledgements This work was partially supported by the DEFEDGE project (E53D23 016380001) under the PRIN program, and the UPSIDE project (B63D23000820004), both funded by the Italian MUR. We express our gratitude to WindTre S.p.A. for their technical support.

References

[Bastian et al., 2023] Bastian, N. B., Bierbrauer, D. B., McKenzie, M. M., and Nack, E. N. (2023). ACI IoT Network Traffic Dataset 2023.

[Beaini et al., 2020] Beaini, P., Elhajj, I., and Kayssi, A. (2020). Gaming Network Traffic Dataset.

[chang Feng et al., 2005] chang Feng, W., Chang, F., chi Feng, W., and Walpole, J. (2005). A traffic characterization of popular on-line games. *IEEE/ACM Transactions on Networking*, 13(3):488–500.

[Chen et al., 2005] Chen, K.-T., Huang, P., Huang, C.-Y., and Lei, C.-L. (2005). Game traffic analysis: An MMORPG perspective. In *Proceedings of the International Workshop on Network and Operating Systems Support for Digital Audio and Video*, pages 19–24, Stevenson Washington USA. ACM.

[Flinck Lindstrom et al., 2020] Flinck Lindstrom, S., Wetterberg, M., and Carlsson, N. (2020). Cloud Gaming: A QoE Study of Fast-paced Single-player and Multiplayer Gaming. In *2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing (UCC)*, pages 34–45, Leicester, UK. IEEE.

[Labayen, 2020] Labayen, V. (2020). Network traffic and code for machine learning classification.

[Labayen et al., 2020] Labayen, V., Magaña, E., Morató, D., and Izal, M. (2020). Online classification of user activities using machine learning on network traffic. *Computer Networks*, 181:107557.

[Labonne et al., 2020] Labonne, M., Chatzinakis, C., and Olivereau, A. (2020). Predicting Bandwidth Utilization on Network Links Using Machine Learning. In *2020 European Conference on Networks and Communications (EuCNC)*, pages 242–247, Dubrovnik, Croatia. IEEE.

[Lyu et al., 2024] Lyu, M., Madanapalli, S. C., Vishwanath, A., and Sivaraman, V. (2024). Network Anatomy and Real-Time Measurement of Nvidia GeForce NOW Cloud Gaming.

[Melo and de Oliveira, 2020] Melo, E. F. and de Oliveira, H. M. (2020). An Overview of Self-Similar Traffic: Its Implications in the Network Design.

[Moon, 2024] Moon, D. (2024). Network Traffic Characteristics and Analysis in Recent Mobile Games. *Applied Sciences*, 14(4):1397.

[Namel et al., 2019] Namel, A. T., Sahib, M. A., and Hasan, S. M. (2019). Bandwidth Utilization Prediction in LAN Network Using Time Series Modeling. *Iraqi Journal of Computer, Communication, Control and System Engineering*, pages 78–89.

[Newzoo, 2024] Newzoo (2024). Global Games Market Report 2024. Technical report. URL: https://newzoo.com/resources/trend-reports/newzoos-global-games-market-report-2024-free-version (accessed: 17/12/2024).

[Rak et al., 2024] Rak, M., Palmiero, P., and Moretta, F. (2024). e-Sport Network Traffic: the UPSIDE dataset.

[Velarde-Alvarado et al., 2022] Velarde-Alvarado, P., Gonzalez, H., Martínez-Peláez, R., Mena, L. J., Ochoa-Brust, A., Moreno-García, E., Félix, V. G., and Ostos, R. (2022). A Novel Framework for Generating Personalized Network Datasets for NIDS Based on Traffic Aggregation. *Sensors*, 22(5):1847.

[Xu et al., 2020] Xu, S., Marwah, M., Arlitt, M., and Ramakrishnan, N. (2020). STAN: Synthetic Network Traffic Generation with Generative Neural Models.