Multi-RAT enhanced Private Wireless Networks with Intent-Based Network Management Automation

Amin Emami, Hilary Frank, Wenhao He, Anderson Bravalheri, Adrian-Cristian Nicolaescu, Haiyuan Li, Hamid Falaki, Shuangyi Yan, Reza Nejabati, and Dimitra Simeonidou

High Performance Networks Research Group, Smart Internet Lab - University of Bristol, UK

***Abstract*—Private wireless networks have become essential enablers for network use cases in enterprises. Emerging enterprise applications push private networks to be more complex in terms of operation and management. However, current private network managers are contending with the challenge of finding a strategy for a network solution that adequately fulfils the service Key Performance Indicators (KPIs) for the growing innovative applications, which are increasingly uplink hungry. They also confront the need to optimise the management of networks without the cost implications associated with hiring onsite experts. In addressing these two key challenges, we demonstrate a multi-connectivity framework that utilises multi-radio access technologies, namely 5GNR, WiFi-6, and LiFi, to enhance private 5G network capacity with intent-based network automation in a museum. Our framework employs MP-TCP link aggregation strategy that combines multiple network connections to ensure a minimum throughput capacity to meet the maximum uplink requirement for a smart tourism pilot use case. As a management enabler, we simplify network service deployment by using an intent-based platform with a Natural Language Processing (NLP) interface. Integrating multi-connectivity and intent-based networking in a private 5G network provides significant advantages for advancing future-generation wireless private networks in research and innovation.**

***Index Terms*—Multi-RAT, multi-connectivity, intent-based networking, private 5G networks, MPTCP, smart tourism, uplink.**

INTRODUCTION

Private wireless networks, especially 5G networks, have emerged as promising solutions to build private enterprise networks by leveraging the advanced capabilities of 5G to enhance wireless connectivity. The interest in deploying private 5G networks has been sparked by the gradual deployment of public 5G networks and the maturation of new network features and functions within these networks.

The straightforward solution is to deploy the available pubic 5G networks to support enterprise applications. However, industries encounter various challenges while attempting to utilize public 5G networks. Some of the obstacles include coverage, security, and network control, which prohibit the adoption of public 5G networks.

Firstly, many industries suffer from inadequate network coverage provided by public network operators. This is because most industries are sited away from residential neighbourhoods, which are the primary targets for subscription by public operators [1]. It is unrealistic to expect the public network operator to provide customized services for all such industries.

Secondly, with rising awareness of privacy breaches and vulnerabilities in complex, virtualised-centric public 5G networks [2], enterprises face increasing challenges in prioritising security against potential malicious exploitation.

Furthermore, there is a growing necessity to exert greater network control due to increasing demands from industrial applications for stringent KPI requirements especially in the uplink, as public networks tend to prioritise downlink applications [15]. These requirements include throughput, latency, reliability, availability, and security [1], which public 5G networks are unable to adequately satisfy.

Enterprises' constraints are driving the adoption of private 5G networks over public alternatives, and recognising their role, the 3rd Generation Partnership Project (3GPP) has termed private 5G network as Non-Public Network (NPN). However, private 5G networks, despite the attraction for enterprise use cases, still face certain challenges. For instance, emerging industry vertical applications demand higher performance standards [2], particularly in areas such as video streaming, IoT data upload, and other similar platforms that involve multicast and broadcast scenarios [14], which rely heavily on uplink capacity. Acknowledging the uplink capacity challenges inherent in public networks, the British Broadcasting Corporation (BBC) deployed standalone private 5G networks for live coverage during the last Commonwealth Games in Birmingham [15].

Inspite of that, private networks still face challenges in handling heavy uplink traffic and delivering high data rates and reliable connectivity over extended coverage with a single radio access technology. [3][4].

Also, the efficient management of private 5G networks by enterprise operators can be problematic. Smaller industries struggle with managing networks efficiently often due to a lack of technical expertise and limited budget [5].

A. *Main contribution*

In this paper, we detailed the implementation of the multi-connectivity testbed supporting two networking functions: i) multi-radio access technologies namely 5G, WiFi-6 and LiFi, and ii) intent-based network management automation, as a management enabler to simplify network operations.

We implemented these via a standalone private 5G network to showcase a smart tourism pilot. Laboratory validation took place at the University of Bristol's Smart Internet Lab, while real deployment testing occurred at the Bristol M-Shed

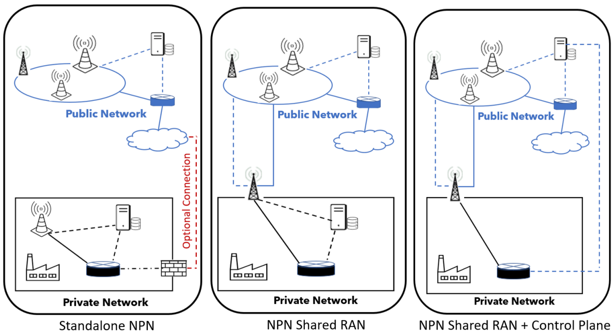


Fig. 1. The primary deployment models of Private 5G Network.

Museum. The experiments highlights performance benefits via link aggregation and user-friendly intent-based network service deployment.

In the subsequent sections, we define key private 5G network requirements, deployment options, introduce our Multi-RAT solution and intent-based network management automation, present experimental measurements and results, and conclude.

I. Overview of Private 5G Networks

Private 5G networks, uses 5G technology, offer dedicated, secure, high-speed connectivity for enterprises. They support diverse use cases, such as enhanced Mobile Broadband (eMBB), Massive Machine-Type Communications (mMTC), and Ultra-Reliable Low-Latency Communications (URLLC) [9].

A. Requirements

Private 5G networks meet diverse application needs with specific characteristics. These include reliability, integration with public networks, high availability, network control, security, and customization [6] [7] [8].

These features ensure private 5G networks can support adequate capacity, network coverage, and resilient service switching functionalities. They also enable seamless integration with public networks, control over configurations decisions, network functions, and traffic flow policies. These features provide end-to-end security and privacy to protect infrastructure, and data, from external threats.

B. Deployment options

The options to deploy private 5G networks are based broadly on two architecture types:

(i) Standalone Non Public Network (SNPN) which is an end-to-end isolated network from the public land mobile network (PLMN); and

(ii) Public Network Integrated-Non Public Network (PNI-NPN), consisting of NPN Shared RAN and NPN Shared RAN + Control Plane. Their deployment is based on a Service Level Agreement (SLA) between the PLMN and private network operator [9]. Figure 1 illustrates the main deployment types for private 5G networks. Further subdivisions of PNI-NPN, not within this paper's scope, are acknowledged. Our experimentation is based on a standalone NPN.

C. Main challenges

High data rate and link reliability are performance requirements, especially in the uplink, that pose obstacles to private 5G networks.

As observed by the authors in [2] [8] and [10], the implementation of an integrated multi-RAT method, application of intent-based/artificial intelligence approaches, utilisation of network slicing and deployment of 5G-capable devices are potential solutions to overcome the challenges faced by enterprise network operators.

Specifically, [8] calls for affordable improvement to private 5G network performance through the integration of WiFi and 5G technologies, as specified by 3GPP in Release 15 and 16 with the introduction of the Non-3GPP Interworking Function (N3IWF).

II. Our deployment solution

Our solution to these challenges addresses the above-mentioned problems in two fronts - the utilisation of a multi-connectivity framework and intent engine deployment.

We designed and built a Customer Premises Equipment (CPE), which is a 5G-enabled device that uses Multi-Path Transmission Control Protocol (MPTCP) to aggregate link capacities of 5GNR, WiFi-6 and LiFi. It provides enhanced bandwidth and link reliability throughout a given coverage area.

We also implement an intent-based service deployment, as a network management enabler. This platform allows non-technical personnel to manage request of intents and deployment of related network services.

A. Multi-connectivity framework

The framework incorporates 5GNR, WiFi-6, and LiFi, within a standalone private network deployment scenario. The objective is to aggregate these multiple network links to provide high data rate with link reliability. The aggregated link will offer sufficient throughput performance to support the required uplink capacity for a smart tourism use case.

1) Multi-connectivity testbed setup: Figure 2 presents the multi-connectivity testbed setup, which comprise of a multi-WAT CPE, a 5G modem, a WiFi-6 module, and a LiFi dongle. All these components are integrated into a single computer board that operates on an MPTCP-enabled Linux kernel [11].

To enable multi-connectivity, each wireless access technology is linked through an individual VLAN and IP subnet configuration. And to establish this connectivity, the MPTCP-enabled CPE is connected to an MPTCP proxy, which is installed in a Virtual Machine (VM) hosted on an edge server, as shown in the figure. The VM, responsible for serving as the MPTCP proxy, possesses an interface that connects to the VLANs and subnetworks associated with 5GNR, WiFi-6, and LiFi. A robot's VNFs establish an indirect connection to the CPE through the MPTCP proxy.

Each of the three access technologies, the CPE, MPTCP proxy and robot VNFs are all connected directly to a management plane responsible for control and management of

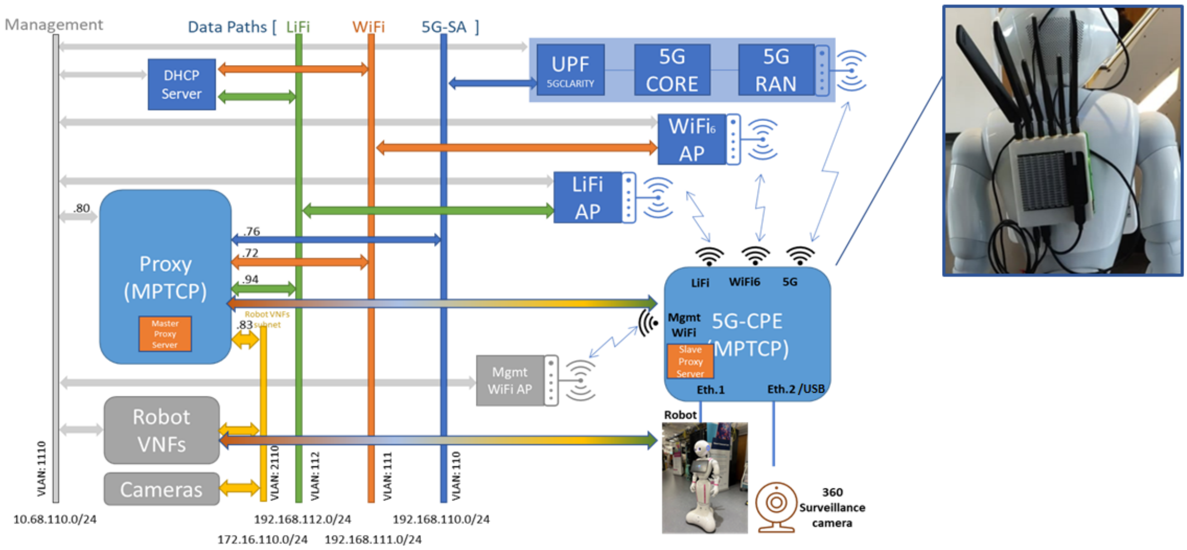


Fig. 2. MPTCP supported multi-connectivity testbed.

the framework.

2) Multi-RAT CPE: The CPE was built at the University of Bristol Smart Internet Lab. It serves as the central hub of the multi-connectivity framework. The device consists of hardware and software components, designed with capability to measure 5G, WiFi-6 and LiFi signals, and connect to the best available link, switch between them and perform throughput aggregation. The use of MPTCP improves the system's reliability by enabling traffic to be routed across the three radio access networks (RANs) through multiple paths.

The CPE, installed on a mobile robot, dynamically switches between 5G, WiFi-6, and/or LiFi wireless access networks as the robot moves. The key functions of the CPE include providing multi-access connectivity, performing multi-connectivity throughput aggregation using MPTCP, conducting handover between different access technologies, and monitoring and measuring key radio parameters and network KPIs.

B. Key infrastructure components

The main components deployed in the smart tourism pilot demonstration are captured in figure 3. The equipment include 5G radio, WiFi-6 and LiFi Access Points (APs). The configurations of these equipment are available in [12]. Other components include a humanoid Pepper robot, on whose body the CPE, the 360-degree camera and a LiFi dongle are attached. The mobility of the robot enables testing of network KPIs at different locations within the coverage area. The CPE performs the measurements, while the 360-degree camera captures surveillance videos for remote monitoring.

The components are integrated in the infrastructure deployed in figure 5. It shows the link between the M-shed museum and Smart Internet Lab sites, each hosting the RAN and Edge clusters respectively. Within the RAN cluster, the multi-RAT access nodes, gNB-CU, and DU are situated. While the Edge cluster houses several compute resources, Virtual Network Functions (VNFs) and the 5G core.

C. Testbed integration and deployment

The deployment stack of our smart tourism experimentation platform consist of the 5G-enabled CPE integrated with MPTCP. A subcarrier spacing of 30 KHz was chosen, and the frame structure type was configured as semi-static.

The WiFi-6 specification operates on the 5.180 GHz frequency. The signal strength for this AP is -40 dBm with an 80MHz configuration.

The LiFi network, takes the form of a pureLiFi-X device, and a LiFi Client, which is a pureLiFi USB dongle. The integration of the various technologies create a multi-connectivity experimentation platform for our smart tourism pilot.

III. Use case description

This section describes the smart tourism pilot use case that utilises our multi-connectivity framework and the scenario that enables its deployment. The use case has been demonstrated at the Bristol M-shed museum in the UK.

The smart tourism pilot comprises two distinct objectives: the implementation of guide robot services in a human-robot

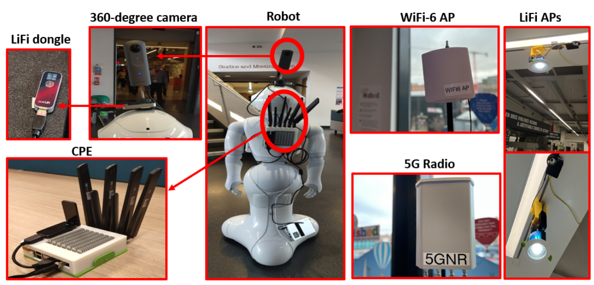


Fig. 3. Key elements of the smart tourism experimentation infrastructure.

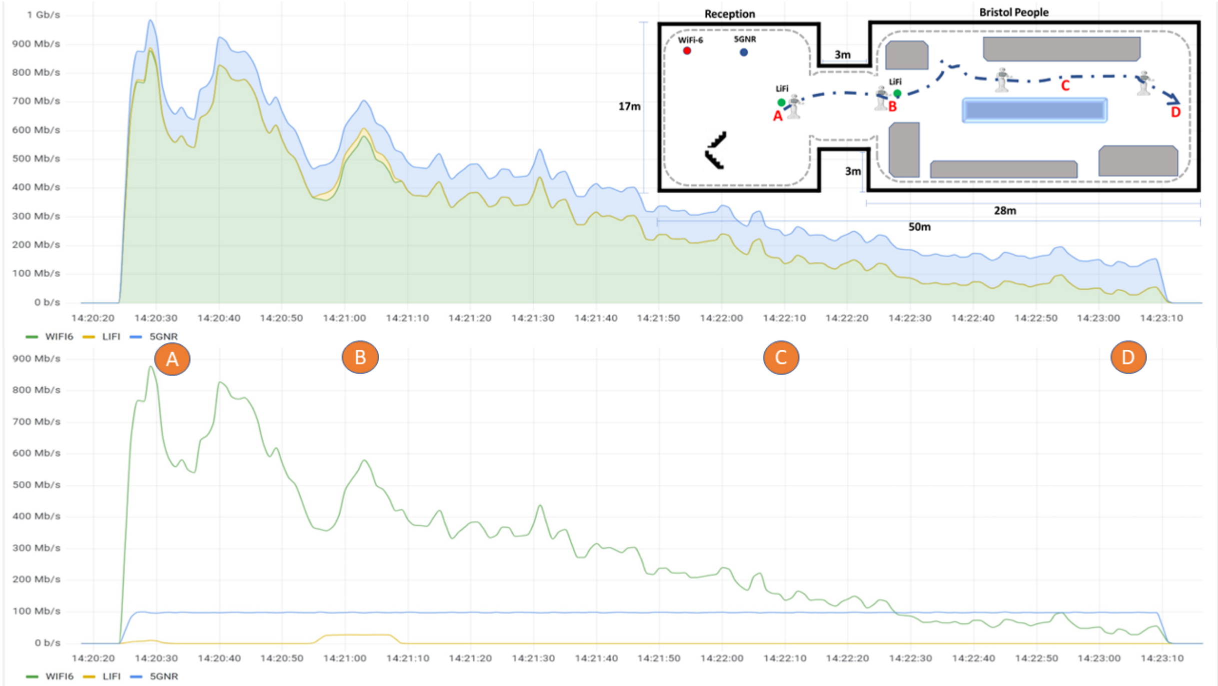


Fig. 4. Multi-RAT Uplink traffic for the cumulative and individual access networks.

interaction scenario, and the remote deployment of surveillance video for public safety monitoring.

In this pilot demonstration, a guide robot service is showcased for museum visitors, enhancing their experience and potentially drawing more tourists. However, the prospect of increased museum visitors raises concern for adequate public safety monitoring. To address this, we integrate a 360-degree camera on the robot to enhance surveillance within the museum environment.

Using the intent engine, a museum safety officer can remotely access on-demand, the surveillance video captured by the 360-degree camera mounted on the robot. Remote access to this footage enhances monitoring and enables prompt intervention when necessary. This ensures a proactive approach to public safety management.

Nevertheless, implementing these advanced functionalities pose some challenges. First, is the demand for high UL bandwidth due to resource-intensive applications. Since a single access network has limitations in meeting the required UL capacity while maintaining network reliability [12], we deployed the CPE, which aggregates the multiple links using MPTCP to achieve the required throughput and network reliability.

IV. Experimental Demonstration

In this section, we describe the experimental demonstration and the methods used to validate the network KPIs.

A. *Methodology*

To determine what wireless capacity would guarantee consistent and reliable coverage for the smart tourism pilot, we performed multiple throughput and latency measurements.

Each round of measurements involved the robot moving from a starting location in the museum labelled location A to the end of the coverage area labelled location D. This measures a total distance of 50 metres. The photo inserted in figure 4 illustrates the described scenario's locations.

B. *Intent-Based Networking*

In the intent-based networking implementation of our smart tourism pilot, the 360-degree footage is streamed to a monitoring device. To achieve this, a streaming server is required to connect the monitoring device. As the safety officer may not possess technical expertise in managing and orchestrating virtualised network functions and services, the intent engine simplifies this network management process by using natural language processing. The safety officer sends an intent request via a web interface specifying the display of video feeds from the 360-degree camera. As a consequence, the service for the intent request is instantiated by description. To deploy this service, a virtual media forwarding unit is set up at the edge of the network.

The intent engine embeds intelligence within the system that enables the instantiation of a machine learning model, serving as a single endpoint. This model is employed by the intent engine, which, upon receiving an intent request, matches it and provides the necessary context information as intent parameters. This context information is needed for identifying the specific Network Service Descriptor (NSD) identifier that requires provisioning. The enterprise services, as defined by the NSD, are then brought onto the Network Function Virtualization Orchestrator (NFVO) and instantiated on the most suitable compute resources in response to the intent request.

C. Network KPI Measurements

Using the CPE, which is mounted on a mobile robot, we collect throughput and latency measurements at various distances from the access points. The reference positions for these measurements are marked in metres (m) as follows: A (0-5m), B (13-15m), C (35-36m), and D (45-50m).

LiFi APs are only at locations A and B. Between both LiFi APs, a signal level discrepancy exists due to the varying heights at which they are installed. Location A has an elevated AP at 4.2 metres, while location B has a lower AP at 2.9 metres, reflecting the different ceiling heights in the building.

The experiment is aimed at benchmarking the UL capacity and investigate the effectiveness of the multi-connectivity framework in meeting the total UL requirement across the coverage area. By saturating the channel, we test the framework's ability to maintain consistent and reliable UL throughput under heavy network traffic conditions. The MPTCP scheduler is set to RoundRobin mode.

V. Results and Analysis

In this section, we discuss the various results from our demonstration, which validates the experiments on intent engine deployment and successfully fulfilled the KPIs for visitor assistance service.

1) Intent Engine Implementation: To implement the service, the museum's safety officer uses natural language to submit intent request. This request triggers the intent engine to instantiate the service, providing a description and requesting the network service (NS) catalogue from the orchestrator (OpenSource MANO). The intent engine then compares the intent description with the catalogue details and returns the identification of the appropriate NS.

The process can be summarized as follows:

(i) Officer initiates intent request using natural language.

(ii) Intent engine generates call logs and creates a network service instance.

(iii) The orchestrator's (OSM) dashboard displays an orange tick to confirm the initialization of the NS instance.

(iv) The OpenStack dashboard indicates the successful instantiation of the Virtual Network Functions (VNFs).

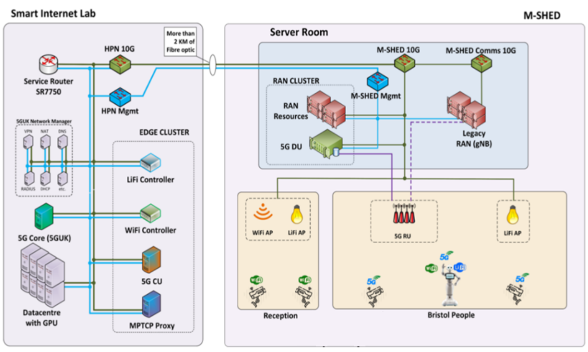


Fig. 5. Connections between the various network infrastructure.

(v) The OSM dashboard verifies the NS instance, changing the ticks to green to indicate its operational status.

(vi) Finally, the requested 360-degree video service is deployed on the safety officer's device.

The visual implementation of the smart tourism pilot is available on YouTube in [13].

A. Throughput Measurements

Figure 4 presents the cumulative and individual throughput of 5G, WiFi-6 and LiFi networks, and the four reference points for measurements.

The upper graph represents the cumulative performance. LiFi and 5G graphs adds on top of WiFi-6 to yield a cumulative performance of about 1 Gbps at location A and 150 Mbps at location D. The yellow contours indicate the contribution of LiFi at locations A and B.

In the lower graph, the individual contributions of 5G, WiFi-6, and LiFi are displayed, showing their respective signal levels across the museum's coverage area. The WiFi-6 signal exhibits fluctuations and its quality diminishes with increasing distance from the AP. Starting at around 890 Mbps, the signal deteriorates and reaches approximately 50 Mbps at location D. For the LiFi, the difference in signal levels between the two APs can be observed, which is due to the disparity in their respective AP height.

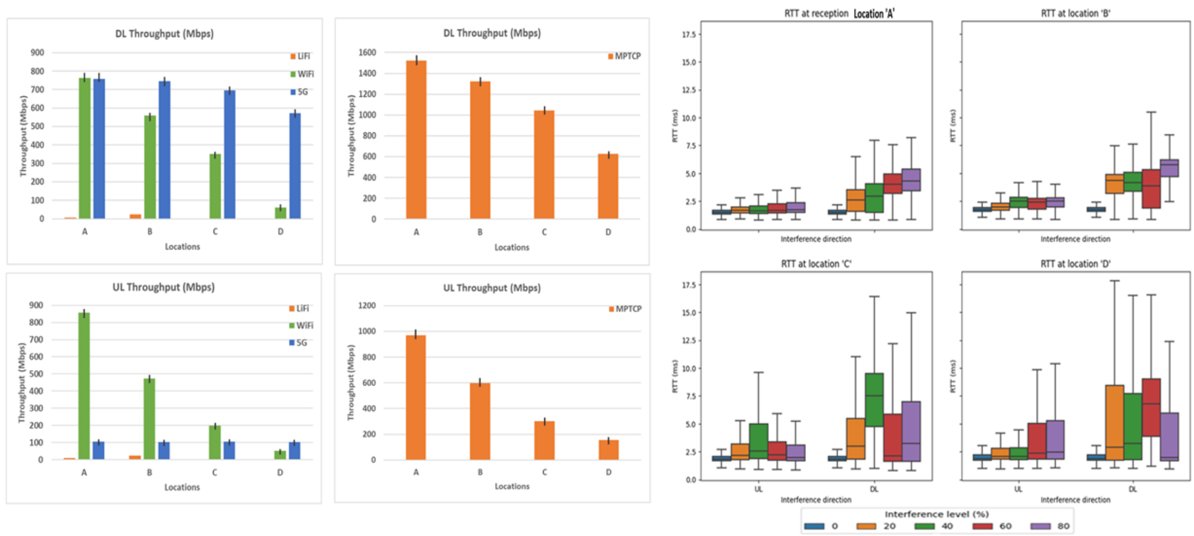
The performance of 5GNR remains consistent across the coverage area, maintaining an average throughput of around 100 Mbps. From locations A to D, we successfully achieved UL throughput above the maximum requirement of 126 Mbps.

Figure 6 (1) Throughput results: Explains the impact of MPTCP on throughput aggregation by showcasing the average throughput performance at locations A, B, C, and D for both UL and DL. A comparison is made between scenarios without MPTCP and those with MPTCP, highlighting the differences in performance. For instance in the UL traffic at location D for both scenarios, the case of MPTCP surpasses the required 126 Mbps. Without MPTCP this would be a struggle. The results from this experiment, highlight the aggregated throughput benefits that multi-RAT implementation can bring to emerging private wireless networks.

We have observed in our multi-connectivity experiments that MPTCP exhibits a performance compensation mechanism. It reacts to a decrease in link capacity as result of a drop in the signal strength in one of the network paths by enhancing the performance of the alternative network path. In our specific case, when the WiFi signal weakens and link throughput decreases accordingly, MPTCP dynamically augments by diverting more traffic to the 5GNR to offset the signal degradation, aiming to meet the quality-of-service requirements, and thereby enhancing overall reliability. This shows an interesting nature of MPTCP that we plan to publish at a later time.

B. Latency Measurements

Figure 6 (2) presents the latency results. At all four locations, the UL traffic encountered lower latency interference compared to the DL traffic. As anticipated, the latency generally rises with increasing distance for both traffic types.



(1) Throughput results (2)Latency results

Fig. 6. Throughput and Latency network KPIs measurement results.

The results confirms that the round-trip time (RTT) stayed below 18 ms for both the UL and DL. This latency level is deemed sufficient for remote control and offloading operations, demonstrating that the network can effectively support these remote video monitoring activities with further prospects for other live streaming broadcast activities without significant delays or interference.

VI. Conclusion

Our multi-connectivity framework demonstrates how Multi-RAT can enhance uplink capacity of private 5G network, while ensuring consistent and reliable connectivity.

The use of intent engine not only simplifies the management of private 5G networks but helps to reduce the operational cost for enterprises operators. This demonstrates the significance of network management automation in facilitating future network service deployments and cost saving for enterprises.

The implementation of both solutions in private wireless networks addresses current challenges of the network and offers a promising experimentation platform for future beyond-5G networks.

Acknowledgements

This work is a contribution by Project REASON, a UK Government funded project under the Future Open Networks Research Challenge (FONRC) sponsored by the Department of Science Innovation and Technology (DSIT). The authors acknowledge the support from the EU - H2020 5G-CLARITY project, grant agreement No. 871428 and EU Horizon H2020 – ICT 2020 5GASP research project, grant agreement No. EP/T017627/1.

References

[1] Wen, M., Li, Q., Kim, K.J., López-Pérez, D., Dobre, O.A., Poor, H.V., Popovski, P. and Tsiftsis, T.A., 2021. Private 5G networks: Concepts, architectures, and research landscape. IEEE Journal of Selected Topics in Signal Processing, 16(1), pp.7-25.

[2] Aijaz, A., 2020. Private 5G: The future of industrial wireless. IEEE Industrial Electronics Magazine, 14(4), pp.136-145..

[3] Mahmoud, H.H.H., Amer, A.A. and Ismail, T., 2021. 6G: A comprehensive survey on technologies, applications, challenges, and research problems. Transactions on Emerging Telecommunications Technologies, 32(4), p.e4233.

[4] Bertizzolo, L., Tran, T.X., Buczek, J., Balasubramanian, B., Jana, R., Zhou, Y. and Melodia, T., 2021. Streaming from the air: Enabling drone-sourced video streaming applications on 5G open-RAN architectures. IEEE Transactions on Mobile Computing.

[5] Mcnamara, J., Camps-Mur, D., Goodarzi, M., Frank, H., Chinchilla-Romero, L., Cañellas, F., Fernández-Fernández, A. and Yan, S., 2023. NLP Powered Intent Based Network Management for Private 5G Networks. IEEE Access.

[6] Eswaran, S. and Honnavalli, P., 2023. Private 5G networks: a survey on enabling technologies, deployment models, use cases and research directions. Telecommunication Systems, 82(1), pp.3-26.

[7] GSMA: IPLOOK — Why Do We Need Private Network? (16 Nov 2021) Online: Accessed 25 Jul 2023. Available https://www.gsma.com/membership/resources/iplook-why-do-we-need-private-network/

[8] Prados-Garzon, J., Ameigeiras, P., Ordonez-Lucena, J., Muñoz, P., Adamuz-Hinojosa, O. and Camps-Mur, D., 2021. 5G non-public networks: Standardization, architectures and challenges. IEEE Access, 9, pp.153893-153908.

[9] Frank, H., Colman-Meixner, C., Assis, K.D.R., Yan, S. and Simeonidou, D., 2022. Techno-economic analysis of 5G non-public network architectures. IEEE Access, 10, pp.70204-70218.

[10] Banda, L., Mzyece, M. and Mekuria, F., 2022. 5g business models for mobile network operators–a survey. IEEE Access.

[11] MPTCP, "MultiPath TCP - Linux Kernel implementation," [Online] Available:https://www.multipath-tcp.org Accessed: 21-05-2023

[12] 5G-CLARITY Deliverable D5.3: Use Cases: Demonstrations and Evaluations [Online] Available:https://www.5gclarity.com/wp-content/uploads/2023/05/5G-CLARITY-D53.pdf. Accessed: 24-06-2023.

[13] 5G-CLARITY Smart Tourism Demonstration. [Online] Available: https://youtu.be/KiMVuBYJ7PA. Accessed: 27-06-2023.

[14] Mi, D., Eyles, J., Jokela, T., Petersen, S., Odarchenko, R., Öztürk, E., Chau, D.K., Tran, T., Turnbull, R., Kokkinen, H. and Altman, B., 2020. Demonstrating immersive media delivery on 5G broadcast and multicast testing networks. IEEE Transactions on Broadcasting, 66(2), pp.555-570.

[15] BBC Research & Development: Using Private 5G Networks for live Commonwealth Games coverage [Online] Available:https://www.bbc.co.uk/rd/blog/2022-08-non-public-5g-networks-broadcasting-production. Accessed: 14-07-2023.