International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

The Role of Edge Computing in Enhancing the Capabilities of Private Wireless Networks

Rahul Bangera

Ellicott City, MD, USA.
rahulmbangera@gmail.com

Abstract:
The convergence of Private Wireless Networks (PWNs), especially those based on the 5G Standalone (SA) architecture and Multi-access Edge Computing (MEC), marks a significant milestone for both the telecommunications and industrial sectors. This research paper provides a detailed technical analysis of how edge computing architectures are essential enablers for Private 5G features, including Ultra-Reliable Low-Latency Communications (URLLC) and enhanced data sovereignty. By thoroughly reviewing 3GPP Releases 16, 17, and 18, particularly regarding Non-Public Networks (NPNs) and the distribution of the User Plane Function (UPF), the study explains how local traffic breakout and deterministic networking function. We compare Private 5G MEC with Wi-Fi 6 in industrial environments, supported by empirical data on latency, jitter, and packet loss. The analysis shows that MEC is not just an addition to Private 5G but a core architectural element necessary to achieve Industry 4.0 goals, highlighting that decoupling the User Plane is the most crucial factor in shifting from consumer broadband to mission-critical industrial connectivity.

Keywords: Private 5G, Multi-access Edge Computing (MEC), Non-Public Networks (NPN), Industry 4.0, URLLC, User Plane Function (UPF), Wi-Fi 6 Comparison, Data Sovereignty, 3GPP Release 18.

I. INTRODUCTION

The industrial landscape is currently undergoing a profound transformation, often referred to as the Fourth Industrial Revolution, or Industry 4.0. The cyber-physical integration of manufacturing processes, autonomous logistics, and data-driven decision-making characterizes this new approach. A key aspect of this shift is the need for widespread, high-performance connectivity that can go beyond the limitations of outdated wired infrastructure and best-effort wireless technologies. While the increase in sensors and the rise of the Industrial Internet of Things (IIoT) have generated large amounts of operational data, the traditional cloud computing model, where data moves through public networks to centralized data centers, has proven insufficient for mission-critical tasks due to inherent latency, jitter, and bandwidth issues [1].
In this context, Private Wireless Networks (PWNs), especially those utilizing 5G New Radio (NR) technology, have emerged as a more effective connectivity option. Unlike public cellular networks designed for consumer mobile broadband, private networks provide enterprises with exclusive spectrum access, detailed Quality of Service (QoS) control, and enhanced security. However, the radio access layer is just one aspect of the solution. To fully leverage the sub-millisecond air interface capabilities of 5G, the computational resources processing the data must be physically and logically closer to where the data is generated. This architectural necessity highlights the importance of Multi-access Edge Computing (MEC) [1].
This paper argues that MEC is crucial to modern private wireless architecture. Without the edge, Private 5G is simply a faster connection; with the edge, it becomes a distributed computing platform capable of supporting real-time, closed-loop control systems. The analysis begins by examining how 3GPP standards have evolved to enable this convergence. Next, it explores the architectural details of the 5G User Plane, specific traffic management methods, and the resulting improvements in latency and bandwidth efficiency.

By comparing these capabilities with Wi- Fi 6, we aim to provide a comprehensive overview of the current state and future direction of this vital technology stack.

II. TECHNICAL FOUNDATIONS AND STANDARDIZATION EVOLUTION

The ability of edge computing to improve private networks is not an accidental outcome but the result of deliberate, rigorous standardization efforts by the 3rd Generation Partnership Project (3GPP) and the European Telecommunications Standards Institute (ETSI). Understanding the development of these standards is key to understanding the reasons and methods behind current deployment models.

A. 3GPP Release 15 and 16: The Architectural Baseline

3GPP Release 15 laid the foundation for the 5G System (5GS) by introducing the Service-Based Architecture (SBA). Importantly, it introduced the concept of Control and User Plane Separation (CUPS). This separated the User Plane Function (UPF) from the control plane, enabling the UPF to be distributed and located at the network edge while the Control Plane remained centralized. This was the key enabler for MEC within the cellular standard [2].

Release 16, finalized in 2020, officially defined support for Non-Public Networks (NPNs). It established two main architectures:

1. **Standalone Non-Public Network (SNPN):** An isolated network with its own Radio Access Network (RAN) and Core Network, separate from public network functions [1].
2. **Public Network Integrated NPN (PNI-NPN):** A dedicated "slice" of a public network.

Release 16 also integrated 5G with IEEE 802.1 Time-Sensitive Networking (TSN) standards, enabling the 5G system to act as a transparent "logical bridge" for Ethernet traffic while maintaining the strict timing required by industrial control protocols [1].

B. 3GPP Release 17 and 18: Edge Enhancements

Release 17 (2022) and the recently frozen Release 18 (2024) have further enhanced edge capabilities. A key addition in Release 17 was the Edge Application Server Discovery Function (EASDF). The EASDF enables the Session Management Function (SMF) to communicate with the DNS system to dynamically direct application requests to the nearest MEC host based on the user's location. This dynamic discovery is essential for mobile robots or Automated Guided Vehicles (AGVs) that may move between different areas of a facility, requiring handovers between various edge nodes [3] [4].

Release 18, marking the beginning of '5G Advanced,' focuses on integrating Artificial Intelligence (AI) and Machine Learning (ML) into the network to improve edge load balancing and support Edge Hosting Environments (EHE). These improvements are essential for enabling seamless roaming and service continuity between private and public edge nodes [4].

C. ETSI MEC Framework

Alongside 3GPP, ETSI defines the application layer framework through the ETSI GS MEC 003 standard. A central aspect of the ETSI/3GPP alignment is the exposure of network information via the Mp1 reference point. Using this interface, an edge application can query the Radio Network Information Service (RNIS) to assess current cell load or radio conditions, enabling it to adjust to network status proactively [5].

III. ARCHITECTURAL FRAMEWORKS OF EDGE-ENHANCED PRIVATE NETWORKS

Deploying an edge computing architecture within a private wireless network is a complex task that requires designing the topology and balancing local processing needs with the costs of distributed infrastructure.

A. The User Plane Function (UPF) as the Gateway

The User Plane Function (UPF) is the crucial support for Protocol Data Unit (PDU) sessions in a Private 5G MEC deployment. In an edge-enhanced architecture, the "Local UPF" is situated at the enterprise premises [2].

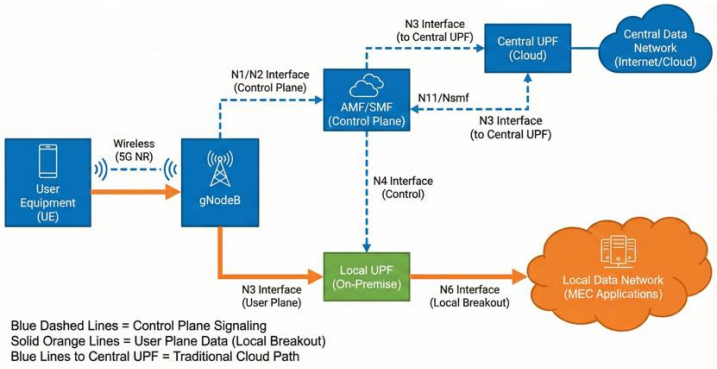

Figure 1: Private 5G network demonstrating local UPF connectivity to MEC applications.

B. Traffic Steering: UL CL and Branching Points

To enable a device to access both local industrial applications and remote internet services simultaneously, 5G uses the Uplink Classifier (UL CL). The UL CL is a feature within the UPF that functions as an intelligent policy router [2].

- **Mechanism:** When a packet arrives from the RAN, the UL CL inspects the header. If the destination IP matches the local MEC server, the packet is forwarded to the local N6 interface. If the destination is the public internet, it is routed through an N9 tunnel to a remote UPF. This ensures that sensitive internal data never leaves the facility's physical perimeter [2].

IV. PERFORMANCE ANALYSIS: LATENCY, DETERMINISM, AND THROUGHPUT

The integration of MEC into Private Wireless Networks is motivated by the need to enhance physical performance metrics: latency (Round Trip Time), jitter (latency variation), and bandwidth efficiency.

A. Latency and Jitter: Edge vs. Cloud

Empirical research comparing edge platforms to centralized cloud platforms measures the performance gap.

- **Latency:** Studies indicate that 5G MEC can achieve median Round Trip Times (RTT) of 11.7 ms, whereas cloud-based routing typically results in 30–50 ms or more [6].
- **Jitter (Stability):** For industrial control, bounded latency is more important than average latency. Research shows that the standard deviation of latency (jitter) for edge connections on 5G is roughly 5 times lower than for cloud connections. This "isochronous" behavior enables 5G to replace cabling in motion-control applications [6].

Table 1: Latency and Jitter Comparison – Edge vs. Cloud [6]

Metric	Private 5G (Local Edge)	Public Cloud (via 5G)	Improvement Factor
Median RTT	~11.7 ms	~48 ms	~4x Lower Latency
Jitter (RTT CV)	0.7%	>5%	~5x Higher Stability
Hop Count	1-2 Hops	10+ Hops	Reduced Complexity

B. Bandwidth Efficiency and Video Analytics

A primary economic driver for Private 5G MEC is the reduction of uplink backhaul demands, especially for video analytics. Sending high-definition video streams from many cameras to a central cloud uses a lot of bandwidth.

- **The MEC Advantage:** By running computer vision algorithms (e.g., object detection) on local MEC nodes, video is processed on-premise. Only metadata (e.g., coordinates of a detected defect) is sent to the cloud [7].
- **Quantitative Impact:** Research shows that this edge-processing model can reduce backhaul bandwidth use by more than 90% compared to raw streaming while maintaining query-level accuracy [7].

C. Comparative Analysis: Private 5G MEC vs. Wi-Fi 6

A common question for industrial CIOs is whether to choose Private 5G or Wi-Fi 6 (802.11ax).

- **Determinism:** Wi-Fi 6 operates in unlicensed spectrum and uses "Listen-Before-Talk" (LBT) mechanisms, which can cause unpredictable delays in noisy industrial environments. 5G uses a centralized scheduler in licensed spectrum, ensuring transmission slots [8].
- **Performance Data:** Recent experimental comparisons using commercial hardware demonstrate that while Wi-Fi 6 can achieve low latency in ideal conditions, its performance degrades significantly under load. 5G LANs have been shown to maintain consistently low packet drop rates and bounded latency even with heavy background traffic, whereas Wi-Fi 6 packet loss spikes due to channel contention [8].

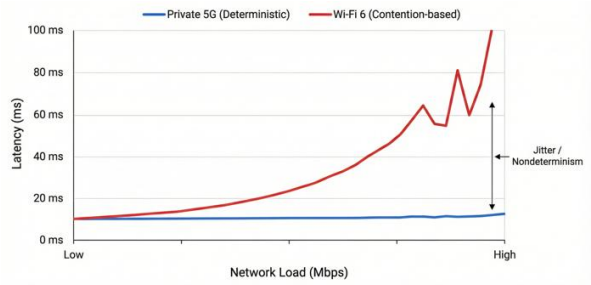

Figure 2: Graph comparing latency with increasing network load for a private 5G and Wi-Fi 6 network.

V. SECURITY, PRIVACY, AND DATA SOVEREIGNTY

Deploying edge resources within a private network fundamentally changes the enterprise's security posture, improving data sovereignty while increasing the threat surface.

A. Data Sovereignty

For industries handling sensitive intellectual property (such as semiconductor manufacturing) or regulated data, the public cloud presents risks of data interception.

- **MEC as a Privacy Shield:** By terminating the PDU session at the local UPF, the enterprise ensures that user payloads never go over the public internet. This setup helps meet strict regulations, such as GDPR. The mobile operator may detect that a device is connected, but the traffic remains local and encrypted (over the air interface and via application-layer protocols) [9] [10].

B. Security Challenges

Decentralizing infrastructure raises vulnerability. Edge nodes, often located in warehouses or outdoor cabinets, are vulnerable to physical tampering. Additionally, the distributed nature of MEC demands careful orchestration to avoid misconfigurations [10].

- **Zero Trust Architecture:** To reduce these risks, a Zero Trust approach is crucial. This includes mutual authentication between edge applications and the core network, as well as network slicing to logically separate different traffic types (e.g., distinguishing security cameras from office Wi-Fi) [10].

VI. FUTURE TRAJECTORIES: TOWARDS 6G AND THE INTELLIGENT EDGE

As the industry advances past the initial deployments of Release 16/17, the roadmap indicates even greater integration of compute and connectivity.

A. Release 18 and 5G Advanced

3GPP Release 18, the first '5G Advanced' standard, introduces a multi-layered AI framework. It incorporates AI/ML directly into the air interface to improve signal reliability (e.g., through intelligent beam management), while also utilizing edge-based AI models to forecast device mobility patterns. For example, the network can analyze an AGV's historical trajectory to pre-allocate radio resources in the target cell, thereby reducing handover latency [11].

B. 6G and the Compute-Continuum

Looking toward 6G, expected around 2030, the line between "Network" and "Computer" will blur. 6G architectures suggest a "Compute-as-a-Service" model where the network functions as a large-scale computing platform, dynamically distributing tasks among the device, the edge, and the cloud based on real-time needs [12].

VII. CONCLUSION

The integration of Multi-access Edge Computing (MEC) into Private Wireless Networks marks a fundamental shift in industrial telecommunications architecture. This research shows that MEC is not just an optional feature but an essential part for realizing the full potential of 5G in enterprise settings. The separation of the User Plane through CUPS and the use of traffic steering mechanisms, such as the Uplink Classifier, enable private networks to overcome the "best-effort" limits of the public internet. As demonstrated by empirical data, combining Private 5G and MEC results in 90% reductions in backhaul bandwidth, a fivefold improvement in latency stability over cloud architectures, and better reliability than Wi-Fi 6 in tough industrial environments. Although security orchestration still faces challenges, the trend is evident: the future of industrial connectivity is private, cellular, and edge-processed.

REFERENCES:

1. M S. Eswaran and P. B. Honnavalli, "Private 5G networks: A survey on enabling technologies, deployment models, use cases and research directions," *Telecommun. Syst.*, vol. 82, no. 1, pp. 3–26, Jan. 2023.
2. *System Architecture for the 5G System (5GS), 3GPP TS 23.501, Version 18.5.0, Release 18, May 2024.*
3. *5G System Enhancements for Edge Computing; Stage 2*, 3GPP TS 23.548, Version 18.6.0, Release 18, Jun. 2024.
4. Qi and C. Herrero-Veron, "Edge computing: 3GPP standards Release 17-19," *3GPP Highlights*, no. 9, Dec. 2024.
5. *Multi-access Edge Computing (MEC); Framework and Reference Architecture*, ETSI GS MEC 003, V3.1.1, Mar. 2022.
6. M. Xu, Z. Fu, X. Ma, L. Zhang, Y. Li, F. Qian, S. Wang, K. Li, J. Yang, and X. Liu, "From cloud to edge: A first look at public edge platforms," in *Proc. ACM Internet Meas. Conf. (IMC)*, Nov. 2021, pp. 37–53.
7. G. Ananthanarayanan *et al.*, "Real-time video analytics: The killer app for edge computing," *IEEE Computer*, vol. 50, no. 10, pp. 58–67, Oct. 2017.
8. V. Sathya, L. Zhang, O. Sahin, and M. Yavuz, "Enterprise approach: Performance analysis of Wi-Fi 6 and 5G private LAN with micro-slicing feature," *IEEE Access*, vol. 12, pp. 119207–119222, 2024.
9. G. Nencioni, R. G. Garroppo, and R. F. Olimid, "5G multi-access edge computing: A survey on security, dependability, and performance," *IEEE Access*, vol. 11, pp. 63496–63536, 2023.
10. S. Y. Shah and M. A. Gregory, "Security in IoT-driven mobile edge computing: New paradigms, challenges, and opportunities," *IEEE Access*, vol. 9, pp. 10903–10924, 2021.

11. *3GPP Release 18 Description; Summary of Rel-18 Work Items*, 3GPP TR 21.918, Release 18, Oct. 2023.
12. M. A. Uusitalo *et al.*, "6G vision, value, use cases and technologies from European 6G flagship project Hexa-X," *IEEE Access*, vol. 9, pp. 160004–160020, 2021.