

Private 5G and Beyond — Networks for IoT

Gautam Sharma¹, Devansh Kulkarni², Satyam Joshi³, Arvind Pratap Singh⁴

Students^{1,2,3}, Professor²

Department of Information Technology

ABES Engineering College

Email ID: *Gautamsharm1aa@gmail.com¹, Kulkarni.1devansh1@yahoo.com², satyam_8joshi@rediffmail.com³*

ABSTRACT

The rapid growth of Internet of Things (IoT) devices in industries, healthcare, agriculture, smart cities, and manufacturing demands communication networks that are reliable, secure, low-latency and scalable. Traditional Wi-Fi and public cellular networks often fail to meet strict industrial and mission-critical IoT requirements. Private 5G networks have emerged as a strong solution by providing dedicated spectrum, ultra-reliable low latency communication (URLLC), enhanced security, and network slicing capabilities. These features make private 5G ideal for industrial IoT, smart factories, autonomous vehicles, and critical infrastructure monitoring. This paper presents a comprehensive review of Private 5G networks for IoT applications and explores how future technologies beyond 5G (B5G/6G) will further enhance IoT connectivity. Architecture, key features, deployment models, use cases, challenges, and future research directions are discussed. The study shows that private 5G combined with edge computing and AI will play an important role in enabling next-generation IoT ecosystems.

KEYWORDS: *Private 5G, IoT, Network Slicing, URLLC, Edge Computing, B5G, 6G, Industrial IoT*

INTRODUCTION

IoT devices are increasing rapidly in number and complexity. From sensors in agriculture to robotic arms in smart factories, these devices generate huge amounts of data and require continuous communication. Existing wireless technologies such as Wi-Fi, Bluetooth, and even

4G LTE are not sufficient for highly reliable and real-time industrial applications.

Private 5G networks offer organizations the ability to deploy their own dedicated cellular infrastructure within a campus, factory, port, mine, or hospital. Unlike public 5G, private 5G gives full control over data, latency, coverage, and security. This makes it very suitable for IoT where predictable performance is required.

Beyond 5G technologies (B5G and upcoming 6G) promise even lower latency, AI-driven networking, terahertz communication, and ultra-massive connectivity which will further enhance IoT applications.

EVOLUTION FROM PUBLIC NETWORKS TO PRIVATE 5G FOR IOT

The journey of wireless communication technologies for IoT has evolved through multiple generations, each trying to address limitations of the previous one. As IoT applications moved from simple sensing to mission-critical automation, the need for more reliable, low-latency, and secure connectivity increased. This evolution gradually shifted focus from public shared networks toward **dedicated private 5G infrastructures** specifically designed for IoT environments.

1. Early IoT Connectivity: Wi-Fi, Bluetooth and ZigBee

In the initial phase of IoT adoption, short-range wireless technologies such as Wi-Fi, Bluetooth, and ZigBee were widely used.

- **Wi-Fi** was preferred due to easy availability and high data rate.
- **Bluetooth and ZigBee** were used for low-power sensor communication.

However, these technologies showed several drawbacks when scaled to industrial or large campus environments:

- Signal interference in crowded spectrum
- Limited coverage and roaming capability
- Unpredictable latency
- Weak security models for critical systems
- Difficulty in managing thousands of devices

These issues became more visible in smart factories, hospitals, and logistics centers where IoT devices needed seamless mobility and consistent performance.

2. Role of 4G LTE in IoT Expansion

4G LTE introduced wider coverage, better mobility management, and more stable connectivity compared to Wi-Fi. It enabled early forms of cellular IoT such as:

- Smart meters
- Asset tracking
- Fleet management

Technologies like **LTE-M** and **NB-IoT** were developed specifically for low-power IoT use cases. While 4G improved IoT deployment, it still had important limitations:

- Latency typically above 30–50 ms, not suitable for real-time control
- Limited device density for massive IoT scenarios
- Dependence on telecom operators and public infrastructure
- Security concerns due to shared network usage

Industrial environments needed deterministic performance which public LTE networks could not guarantee.

3. Emergence of Public 5G Networks

Public 5G networks introduced significant improvements:

- Ultra-Reliable Low Latency Communication (URLLC)
- Massive Machine Type Communication (mMTC)
- Enhanced Mobile Broadband (eMBB)

These features were attractive for IoT, especially for video analytics, robotics, and automation. But public 5G still operates on **shared spectrum and shared infrastructure**, which means:

- Bandwidth is shared with consumer users
- Network performance may vary during peak hours
- Data leaves the organization's premises
- Limited customization of network parameters

This made enterprises realize that although 5G technology is capable, **public 5G deployment model is not ideal for sensitive IoT operations.**

4. Shift Toward Private Cellular Networks

To overcome the limitations of public networks, organizations started exploring **private LTE** and later **private 5G** networks. Regulatory bodies in many countries opened dedicated spectrum bands (such as CBRS in the USA) for private use.

Private cellular networks provided:

- Dedicated spectrum for enterprise
- Local deployment of base stations
- Control over Quality of Service (QoS)
- Better data privacy and governance

This was the turning point where industries began migrating from Wi-Fi and public LTE toward private cellular solutions.

Table 1: Why Private 5G is a Natural Fit for Modern IoT

Technology	Key Limitation for IoT	Improvement in Private 5G
Wi-Fi	Interference, limited coverage, poor mobility	Dedicated spectrum, seamless mobility
4G LTE	Higher latency, limited device density	URLLC, massive IoT support
Public 5G	Shared bandwidth, security concerns	Dedicated control, custom configuration
LPWAN (LoRa, Sigfox)	Low data rate	High data rate + low latency

Private 5G combines advantages of cellular reliability with local control.

ARCHITECTURE OF PRIVATE 5G FOR IOT

The architecture of a Private 5G network for IoT is designed to provide **low latency, high**

reliability, data privacy, and local control. Unlike public cellular networks where most intelligence resides in the operator's core, private 5G pushes key functions inside the enterprise premises. This allows organizations to tightly integrate IoT devices, compute resources, and network control into a single managed ecosystem.

A typical private 5G IoT architecture consists of five major components:

1. **IoT Devices and Sensors**
2. **5G Radio Access Network (gNodeB)**
3. **Local 5G Core**
4. **Edge Computing Server**
5. **Cloud / Enterprise Network**

These components work together to create an end-to-end communication and processing pipeline optimized for IoT workloads.

1. IoT Devices and Sensors

This layer includes all field devices that generate or consume data:

- Environmental sensors (temperature, humidity, gas, vibration)
- Cameras for surveillance and vision inspection
- Industrial robots and PLC-connected machines
- Wearables and handheld terminals
- Autonomous Guided Vehicles (AGVs) and drones

These devices are equipped with **5G modules or gateways** that allow them to directly connect to the private 5G network using SIM/eSIM authentication.

Key characteristics:

- Large number of devices (mMTC scenario)
- Mobility support for moving devices
- Low power consumption for battery devices
- Secure identity using SIM credentials

2. 5G Radio Access Network (gNodeB)

The **gNodeB** is the 5G base station that provides wireless connectivity to IoT devices. Multiple

small cells may be deployed across a factory floor, hospital campus, port, or warehouse to ensure full coverage.

Functions of gNodeB:

- Radio signal transmission and reception
- Device scheduling and radio resource management
- Mobility and handover management
- Traffic prioritization based on network slices

In private setups, gNodeBs are strategically placed indoors and outdoors to avoid dead zones and interference common in Wi-Fi deployments.

3. Local 5G Core

The **local 5G core** is the most important differentiator of private 5G. Instead of routing traffic to a telecom operator's core, the enterprise hosts its own 5G core functions on-premise.

Core components include:

- AMF (Access and Mobility Management Function)
- SMF (Session Management Function)
- UPF (User Plane Function)
- AUSF (Authentication Server Function)
- PCF (Policy Control Function)

Benefits:

- Data remains inside the premises
- Ultra-low latency due to local routing
- Full control over QoS policies
- Custom network slicing for IoT applications

4. Edge Computing Server

Edge servers are placed very close to the 5G core to process IoT data in real time.

Role of edge computing:

- AI/ML inference on video streams

- Real-time control for robots and machines
- Local data analytics and filtering
- Reduced backhaul to cloud
- Faster decision-making

For example, a vision inspection camera sends video via 5G to the edge server where AI detects defects instantly without sending data to the cloud.

5. Cloud / Enterprise Network

The cloud or enterprise data center is used for:

- Long-term data storage
- Model training for AI systems
- Enterprise applications (ERP, SCADA, dashboards)
- Remote monitoring and management

Only processed or necessary data is forwarded from edge to cloud, optimizing bandwidth usage.

KEY FEATURES OF PRIVATE 5G BENEFICIAL FOR IOT

Private 5G is designed not just as a faster wireless network, but as a **deterministic, secure, and highly scalable communication platform**. These features directly match the demanding requirements of IoT environments such as factories, hospitals, ports, mines, and smart campuses. The following core capabilities make private 5G highly suitable for mission-critical IoT deployments.

1. Ultra-Reliable Low Latency Communication (URLLC)

URLLC is one of the most important service categories defined in 5G. It ensures:

- **Extremely low latency** (as low as ~1 ms in local deployments)
- **Very high reliability** (packet delivery success > 99.999%)
- **Deterministic performance** even under heavy load

In IoT environments, many applications cannot tolerate delay or packet loss.

Examples:

- Real-time robotic arm control in smart factories
- Motion control for CNC machines
- AR/VR headsets for maintenance guidance
- Remote operation of cranes in ports
- Telesurgery assistance in hospitals

Older technologies like Wi-Fi or LTE may introduce unpredictable delays due to contention or congestion. Private 5G with URLLC ensures guaranteed response time, which is critical for automation.

2. Massive Machine Type Communication (mMTC)

IoT deployments often include **thousands of sensors** in a limited area. mMTC is designed to handle this scale efficiently.

Capabilities:

- Support for very high device density per square kilometer
- Efficient signaling for low-power devices
- Optimized bandwidth usage for small data packets
- Long battery life for IoT sensors

Examples:

- Smart agriculture fields with soil and weather sensors
- Smart buildings with lighting, HVAC, and occupancy sensors
- Industrial plants with vibration, temperature, and pressure sensors everywhere

Traditional networks struggle when too many devices connect simultaneously. Private 5G manages device access intelligently without congestion.

3. Network Slicing

Network slicing allows the creation of multiple **virtual networks** on the same physical 5G infrastructure. Each slice can be configured with its own QoS, latency, and bandwidth settings.

Why this matters for IoT:

Different IoT applications have different requirements.

Table: 2

IoT Application	Requirement	Network Slice Configuration
CCTV video analytics	High bandwidth	eMBB slice
Sensors	Low data, long battery	mMTC slice
Robot control	Ultra-low latency	URLLC slice

This ensures that heavy video traffic does not affect control signals of robots or sensor data transmission.

4. Enhanced Security

Security is a major concern in IoT because many devices are vulnerable to attacks. Private 5G provides a strong security framework:

- **SIM/eSIM-based authentication** for every device
- End-to-end encryption of data
- Isolated private network not accessible from public internet
- Centralized policy control through 5G core
- Support for zero-trust security models

Unlike Wi-Fi passwords that can be shared or hacked, SIM credentials uniquely identify each IoT device, making unauthorized access very difficult.

5. Mobility Support

In many IoT environments, devices are not static. Examples include:

- Autonomous Guided Vehicles (AGVs) in warehouses
- Drones for inspection
- Wearable devices for workers
- Moving robots in production lines

Private 5G provides **seamless handover** between gNodeBs without connection drop. This is a big limitation in Wi-Fi networks where roaming often causes delay or packet loss.

DEPLOYMENT MODELS OF PRIVATE 5G

Table: 3

Model	Description	Suitable for
Fully On-Premise	Entire 5G core and RAN inside campus	Factories, defense
Hybrid Model	Core on cloud, RAN on site	Hospitals, campuses
Network as a Service	Managed by telecom operator	Enterprises without expertise

INTEGRATION OF EDGE COMPUTING WITH PRIVATE 5G

Edge computing processes IoT data near source. Combining edge with private 5G:

- Reduces backhaul traffic
- Enables real-time analytics
- Supports AI inference locally
- Improves privacy

Example: Vision inspection in manufacturing using edge AI.

USE CASES OF PRIVATE 5G IN IOT

1. Smart Manufacturing (Industry 4.0)

Robotic control, predictive maintenance, digital twins.

2. Smart Healthcare

Connected ambulances, remote surgery assistance, patient monitoring.

3. Smart Agriculture

Drone monitoring, soil sensors, irrigation automation.

4. Smart Ports and Logistics

Automated cranes, asset tracking, autonomous trucks.

5. Mining and Oil Fields

Remote monitoring in hazardous areas.

CHALLENGES IN PRIVATE 5G IOT DEPLOYMENT

- High initial deployment cost
- Spectrum licensing issues

- Device compatibility
- Skilled workforce requirement
- Integration with legacy systems

BEYOND 5G (B5G) AND 6G FOR IOT

Future technologies will enhance IoT networking:

Table: 4

Feature	5G	B5G / 6G
Latency	~1 ms	<0.1 ms
Spectrum	Sub-6 GHz, mmWave	Terahertz
Intelligence	Limited AI	AI-native networks
Device Density	High	Ultra-massive
Positioning	Meter level	Centimeter level

6G will support holographic communication, digital twins, and intelligent environments.

SECURITY AND PRIVACY CONSIDERATIONS

Private 5G improves security but still faces:

- Insider threats
- IoT device vulnerabilities
- Need for continuous monitoring
- Zero-trust architecture adoption

COMPARISON: PRIVATE 5G VS WI-FI 6/7 FOR IOT

Table: 5

Parameter	Private 5G	Wi-Fi 6/7
Coverage	Large area	Limited
Mobility	Excellent	Moderate

Parameter	Private 5G	Wi-Fi 6/7
Latency	Very low	Low
Security	SIM-based	Password-based
Device Density	Very high	Moderate

FUTURE RESEARCH DIRECTIONS

- AI-driven network slicing
- Energy-efficient private 5G nodes
- Integration with satellite IoT
- Blockchain for trust management
- 6G enabled tactile IoT

CONCLUSION

Private 5G networks are transforming IoT communication by providing dedicated, reliable, and secure connectivity. They overcome the limitations of traditional wireless technologies and support mission-critical IoT applications across industries. When integrated with edge computing and AI, private 5G enables real-time analytics and automation. Looking ahead, B5G and 6G technologies will further enhance IoT with ultra-low latency, intelligent networking, and massive connectivity. Despite challenges such as cost and spectrum management, private 5G is expected to become the backbone of industrial IoT and smart infrastructure in coming years.

REFERENCES

1. A. Gupta et al., "Private 5G Networks for Industrial IoT," IEEE Communications Magazine, 2022.
2. S. Chen and J. Zhao, "The Requirements, Challenges, and Technologies for 5G of IoT," IEEE Network, 2021.
3. M. Series, "IMT Vision for 2020 and Beyond," ITU Report, 2020.
4. P. Popovski et al., "Wireless Access for Ultra-Reliable Low-Latency Communication," IEEE Network, 2019.
5. N. H. Mahmood et al., "White Paper on 6G Networking," 6G Flagship, 2021.
6. Ericsson, "Private 5G for Enterprises," White Paper, 2022.

7. Nokia, "Edge Computing and Private Wireless," Technical Report, 2023.
8. 3GPP TS 23.501, "System Architecture for 5G," Release 16.
9. K. Zheng et al., "Smart Factory using 5G IoT," Future Internet Journal, 2022.
10. L. U. Khan et al., "6G Wireless Systems: Vision and Applications," IEEE Access, 2021.