Computer Communications 242 (2025) 108295

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Review

Private networks: Evolution, ecosystem, use cases, architecture, spectrum, and deployment challenges

Onur Sahin [a,*], Vanlin Sathya [b], Mehmet Yavuz [b]

[a] Izmir Turk College, Izmir, Turkey
[b] Celona, Campbell, CA, United States of America

ARTICLE INFO

Keywords:
Private networks
Private 5G
Private 6G
Spectrum sharing

ABSTRACT

Private networks have reshaped enterprise communications by providing unmatched control, security, and tailored solutions for various industries. This paper presents an in-depth survey of private networks, covering their evolution, current landscape, and future outlook. Key topics include the use cases, architecture, spectrum management, and deployment strategies. The study examines the transition from private 4G/LTE to private 5G networks, fueled by demands for higher data throughput and ultra-low latency across sectors. It highlights the advantages of private 5G over public mobile networks (MNOs) and Wi-Fi, with a special focus on spectrum sharing as a means to optimize frequency use. Additionally, the paper reviews global spectrum allocations for private 5G, providing an overview of regulatory frameworks and available frequency bands across countries. It also explores future prospects, including private 6G networks and emerging spectrum technologies. Key challenges such as high deployment costs, interoperability issues, and security concerns are discussed alongside potential solutions. Through this comprehensive analysis, the paper aims to provide valuable insights for researchers, practitioners, and policymakers in the field of private networks.

Contents

* Corresponding author.
E-mail addresses: onursahin721@gmail.com (O. Sahin), vanlin@celona.io (V. Sathya).

https://doi.org/10.1016/j.comcom.2025.108295
Received 16 November 2024; Received in revised form 4 July 2025; Accepted 3 August 2025
Available online 16 August 2025

1. Introduction

Private networks are wireless communication systems specifically designed to serve the exclusive needs of a particular organization or industry, offering dedicated connectivity separate from public cellular or Wi-Fi networks. Unlike public networks that cater to a vast user base with shared resources, private networks deliver tailored performance, security, and control to address specific industrial and enterprise demands. A critical distinction between private and public networks lies in ownership and access: while public networks are managed by mobile network operators (MNOs) and accessible by the general public, private networks are typically deployed by enterprises directly or in collaboration with MNOs, allowing them to customize and secure the network environment for operational needs. Increasingly, industries such as manufacturing, logistics, and healthcare are turning to private networks to automate processes and connect devices seamlessly, especially where real-time machine-to-machine communication is essential for efficiency and precision. Fig. 1 shows a typical private network architecture. Devices equipped with private SIMs connect to a dedicated Radio Access Network (RAN), which links to the Edge computing layer for processing. Finally, an Artificial Intelligence/Machine Learning (AI/ML)-powered Orchestrator manages network resources and optimizes performance dynamically.

As industries embrace automation, there is a growing reliance on machinery, robots, and autonomous systems to reduce human error and increase operational accuracy. Within factories, for example, forklifts, automated guided vehicles, and robotic arms require consistent, high-speed connectivity to operate without interruptions. Conventional Wi-Fi and public mobile networks often struggle to provide adequate signal strength and reliability, particularly in enclosed industrial spaces where interference and weak signal penetration can compromise performance. This need for reliable connectivity has driven demand for private networks that operate on dedicated cellular protocols, supported by private cellular infrastructure like access points (APs), edge computing, and secure data channels. With these setups, private networks empower industries to achieve high-performance, uninterrupted connectivity, supporting real-time applications and ensuring that automation processes run smoothly and effectively.

The advent of private networks has revolutionized the communication landscape, offering unprecedented control, security, and customization for enterprises and organizations. Unlike public networks managed by large telecommunications companies, private networks are tailored to meet specific needs, providing dedicated bandwidth,

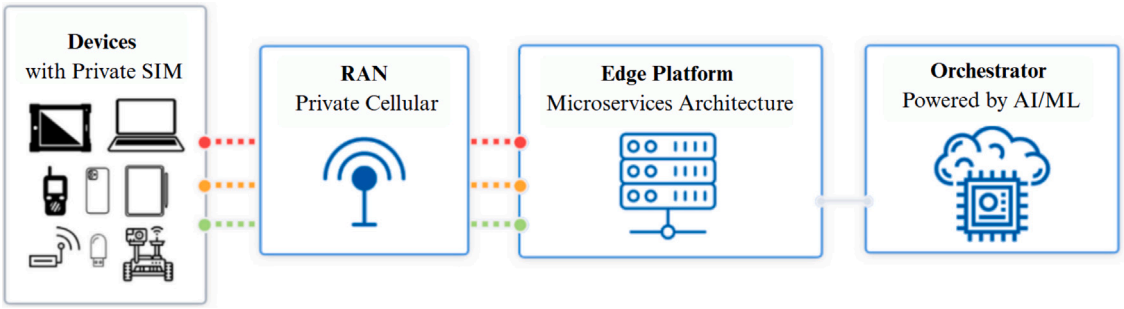

Fig. 1. Architecture of a private network solution.

enhanced security, and improved performance. This paper aims to explore the evolution of private networks, their current state, and future prospects, highlighting their significance in the modern communication ecosystem.

1.1. Background and motivation

The development of private networks accelerated as the Federal Communications Commission (FCC) released spectrum for commercial use, notably establishing the Citizens Broadband Radio Service (CBRS) in 2015. This initiative opened the 3.5 GHz band (3550–3700 MHz) for shared commercial access with a three-tier model: Incumbent Access, Priority Access License (PAL), and General Authorized Access (GAA), promoting efficient spectrum use. The CBRS framework, developed over several years by the FCC and the Wireless Innovation Forum (WInnForum), marked a milestone in regulatory practices [1,2].

Early private 4G/LTE networks focused on basic communication needs, with limited data requirements primarily supporting sectors like utilities and transportation. These networks handled tasks such as remote monitoring and field communication, where high data throughput was not critical [3,4]. As technology advanced, private 4G networks expanded to support more complex use cases driven by industry digitalization. What began as simple communication frameworks quickly adapted to data-intensive applications [5–7].

A significant shift involved using high-resolution cameras in industrial settings for surveillance, remote inspections, and quality control [8,9]. Smart sensors and IoT devices further pushed the limits in manufacturing, continuously monitoring production metrics and environmental data in real-time, which began to exceed the capacity of 4G networks [8]. The transportation sector embraced connected vehicle technology, enabling real-time fleet communication, traffic updates, and diagnostics, which underscored the bandwidth constraints of 4G [10]. In healthcare, telemedicine evolved from simple video consultations to advanced services requiring high-quality video and remote diagnostics, challenging the data and latency limits of 4G [11,12].

Public safety agencies also expanded 4G usage with body-worn cameras, real-time emergency data sharing, and analytics. However, network congestion during emergencies limited effectiveness [12]. In agriculture, precision farming with drones, automated equipment, and IoT sensors required real-time data handling, revealing further bandwidth and latency issues [11,13]. The surge in connected devices and IoT applications exacerbated these limitations, revealing the need for a more robust solution [12]. This demand led to increased interest in private 5G networks, which offer enhanced bandwidth, speed, and capacity ideal for modern data-heavy applications. Private 5G supports high-resolution data streaming, real-time processing, and robust connectivity across industries like manufacturing, healthcare, logistics, and agriculture, addressing the limitations of 4G while promoting efficiency and innovation [11].

Private networks provide industry-specific solutions, enhancing machine-to-machine communication for industrial automation [14–18]. In healthcare, they secure patient data transmission and telemedicine [19–21]. In logistics, private networks enhance tracking and supply chain management [22–27]. The growing interest in private networks is also fueled by advancements in 5G technology. 5G networks promise higher data rates, ultra-low latency, and massive connectivity, making them ideal for private network applications. Enterprises are increasingly deploying private 5G networks to leverage these capabilities for mission-critical applications [28]. Recent studies have shown a significant increase in the number of private network deployments globally. Countries like Germany and Japan have taken proactive steps in allocating spectrum specifically for private network use, recognizing their potential to drive innovation and economic growth [29,30]. This global trend underscores the critical role private networks play in the digital transformation of industries.

1.2. Contribution of our paper

This survey paper provides a comprehensive analysis of the state of private networks, focusing on various critical aspects that are essential for understanding and advancing this field. The key contributions of our paper are as follows:

- Examination of both private 4G/LTE and private 5G networks, highlighting their features, benefits, and implementation challenges.
- Extensive analysis of in-depth use cases for private 5G networks, showcasing practical applications and their impact on various industries.
- Comprehensive review of spectrum sharing and availability across different countries, providing a global perspective on regulatory and operational considerations.
- Discussion on architectural models for private networks, including both standalone and non-standalone configurations.
- Exploration of future spectrum needs and trends, addressing the requirements for advancing private network technologies.
- Overview of devices specifically designed for private 5G networks, evaluating their capabilities and market availability.
- Insight into prospective private 6G networks, discussing the potential advancements and future directions.

These contributions collectively provide a holistic view of private network technologies, offering valuable insights for researchers, practitioners, and policymakers involved in this evolving domain.

To guide the reader, the remainder of this paper is organized as follows: Section 2 presents a review of related works in the field of private 5G and spectrum sharing. Section 3 discusses global spectrum allocations for private 5G deployments. Section 4 covers various architectures used for private deployments. Section 5 highlights the advantages of private 5G over MNOs and Wi-Fi. In Section 6, we explore real-world use cases for private networks utilizing spectrum sharing. Section 7 identifies key challenges in private 5G deployments and outlines potential mitigation strategies. Section 8 discusses the future outlook of private networks. Finally, Section 9 concludes the paper and suggests directions for future work.

2. Related works

This section provides an overview of existing research on private networks, CBRS, spectrum sharing, and network architectures, followed by a comparative analysis of existing survey papers on private networks. This comprehensive review aims to highlight the current state of research, identify gaps, and position the novelty of our survey paper.

2.1. Private networks

Private networks have garnered significant attention in recent years due to their potential to offer secure, high-performance connectivity tailored to specific organizational needs.

Bektas et al. (2021) present a framework for the rapid planning of temporary private 5G networks using unsupervised machine learning. This approach addresses the challenges of antenna placement and regulatory compliance, ensuring guaranteed quality of service in ad-hoc deployments. The framework quickly and autonomously determines optimal antenna positions and power levels for various scenarios, demonstrating its effectiveness in realistic private 5G network environments [31].

This study by Kim et al. (2022) proposes a neural 5G traffic generation model and a spectrum requirement calculator for private 5G networks. It utilizes a generative adversarial network (GAN) to generate realistic traffic based on actual data traces and probability-based models for industrial applications. The spectrum requirements are calculated using both frequency division duplexing (FDD) and time division duplexing (TDD), with simulations showing a bandwidth requirement ranging from 22.0 MHz to 397.8 MHz depending on the deployment scenario. This work is relevant for providing advanced wireless connectivity across various industrial verticals and offers a detailed methodology for accurate spectrum calculation [32]. Bektas et al. (2021) examine the advantages of demand-based planning and configuration for private 5G networks. They showcase a 5G-powered racing platform, demonstrating different 5G Standalone Time Division Duplex patterns for event-driven scenarios. The study highlights the benefits of such configurations and proposes future explorations using machine learning for live planning and network parameterization [33].

Brown (2019) explores the advantages of private 5G networks for industrial IoT, emphasizing their ability to meet the coverage, performance, and security requirements of Industry 4.0 applications. The paper discusses how private 5G networks can optimize business processes and address demanding industrial applications through innovations in 5G technology, including network slicing and ultra-reliable low-latency communications. The research highlights the importance of spectrum availability and effective deployment strategies for the success of private 5G networks in various industrial sectors [15]. The study by Bavikatti et al. [34] evaluates the performance of a private 5G standalone campus network at Technische Universität Kaiserslautern, focusing on download/upload speeds, latency, and signal strength in various environments. It reveals a gap between advertised and actual data rates, influenced by factors such as cell load and network software versions, offering insights for optimizing private 5G network deployments.

The 5G CONNI project investigates innovative solutions for private 5G networks and beyond, focusing on future smart factories leveraging Industry 4.0 and 5G technologies. The project aims to define new architectures, develop advanced technologies, and validate these through a cross-continental industrial private 5G network demonstration between Taiwan and Europe. This research highlights the critical role of private 5G networks in meeting the specific and challenging requirements of industrial applications [35]. The article by Aijaz provides a comprehensive technical overview of private 5G networks, emphasizing their importance in the digital transformation of industrial systems driven by Industry 4.0 and Industrial Internet initiatives. It discusses the concept and functional architecture of private 5G, highlighting key benefits and industrial use cases. The paper also explores spectrum opportunities for private 5G networks, design aspects, and key challenges, along with emerging standardization and innovation ecosystems [36].

2.2. Survey paper comparison

Table 1 presents a comparative analysis of our paper and all existing survey papers on private networks. This comparison highlights the scope and focus areas of each publication, covering aspects such as private 4G/LTE implementations, private 5G architectures, detailed use cases, spectrum sharing mechanisms, architecture models, future spectrum needs, and prospective private 6G developments.

Eswaran and Honnavalli [28] provide comprehensive and detailed coverage of private 5G networks with extensive analysis of architecture models, particularly focusing on Standalone (SA) and Non-Standalone (NSA) deployment scenarios. Their work includes thorough technical specifications, performance metrics, and implementation guidelines for private 5G systems. While they briefly touch upon use cases for private 5G applications in industrial settings, their treatment of spectrum sharing considerations remains limited to basic CBRS framework discussion, and future spectrum needs are only superficially addressed. Notably, their survey completely omits private 4G/LTE implementations, which remain crucial for many industrial deployments seeking gradual migration paths, and provides no coverage of device ecosystems for private 5G or prospective private 6G developments.

Angin et al. [37] focus specifically on private 5G networks within the European regulatory context, providing detailed security analysis and threat assessment frameworks with brief mention of industrial and enterprise use cases. Their work emphasizes privacy protection mechanisms and data security protocols specific to European GDPR compliance requirements. However, their survey does not cover spectrum sharing mechanisms, architectural deployment models (SA/NSA), future spectrum allocation needs, private 4G/LTE legacy systems, device compatibility considerations for private 5G, or emerging private 6G technologies and their potential applications.

M. Wen et al. [38] provide a thorough and comprehensive examination of private 5G networks, covering technical architectures, deployment strategies, and performance optimization techniques while briefly addressing industrial use cases, spectrum sharing considerations within the CBRS framework, and basic architectural models including edge computing integration. Their work includes detailed analysis of network slicing, quality of service guarantees, and interference management. However, their survey does not explore future spectrum allocation requirements, private 4G/LTE legacy system integration, comprehensive device ecosystem analysis for private 5G, or prospective private 6G developments and their implications for enterprise deployments.

Wang and Jain [39], in their unpublished work, briefly mention private 5G network fundamentals and basic spectrum sharing approaches within the United States regulatory framework. Their preliminary analysis touches on deployment considerations and cost-benefit assessments for enterprise applications. However, their survey lacks depth and does not cover detailed industrial use cases, comprehensive architecture models, future spectrum allocation needs, private 4G/LTE system considerations, device compatibility analysis for private 5G implementations, or future private 6G technology roadmaps and their potential impact on private networking.

Prados-Garzon et al. [40] provide comprehensive and detailed coverage of private 5G networks, including extensive technical analysis of network architectures, deployment models, and performance optimization strategies while briefly addressing enterprise and industrial use cases and basic architectural models including SA/NSA considerations. Their work includes thorough examination of network function virtualization, software-defined networking integration, and quality of service mechanisms. However, their survey does not explore spectrum sharing mechanisms, future spectrum allocation requirements, private 4G/LTE legacy system integration, comprehensive device ecosystem coverage for private 5G, or future private 6G developments and their technological implications.

Table 1
A comparison of all existing private network survey papers.

Ref.	Year	Published in	Private 5G	Detailed use cases for private 5G	Spectrum sharing and global availability	Arch models (SA/NSA)	Future spectrum needs	Private 4G/LTE	Devices for private 5G	Future private 6G
Eswaran and Honnavalli [28]	2022	Springer Telecom-munication Systems	✓	△	△	✓	△			
Angin et al. [37]	2022	ICT ReBICTE	✓	△						
M. Wen et al. [38]	2022	IEEE JSTSP	✓	△	△	△				
Wang and Jain [39]	2021	Not Published	△		△					
Prados-Garzon et al. [40]	2021	IEEE Access	✓	△		△				
Maman et al. [41]	2021	J Wireless Com Network	✓	✓	✓	✓				△
Patwary et al. [42]	2022	IEEE Access	✓		✓		✓			✓
Scalise et al. [43]	2025	Future internet	△			△				
This survey paper	2024	Not published	✓	✓	✓	✓	✓	✓	✓	✓

Note:
1. The ✓ symbol indicates that the aspect is covered in detail in the reference.
2. The △ symbol means that this aspect is only mentioned briefly or with other contents but not discussed comprehensively in a single section in the reference.
3. A blank means that this aspect is not covered at all in the reference.

Maman et al. [41] offer detailed and comprehensive analysis of private 5G networks, including extensive coverage of industrial and enterprise use cases, thorough spectrum sharing considerations within multiple regulatory frameworks, and comprehensive architecture models encompassing both technical and business perspectives. Their work provides in-depth analysis of deployment strategies, cost optimization, and performance benchmarking across various industry verticals. While they briefly touch upon future private 6G developments from a conceptual standpoint, their survey does not address future spectrum allocation needs, private 4G/LTE legacy system integration, or comprehensive device ecosystem analysis for private 5G networks.

Patwary et al. [42] thoroughly examine private 5G networks with comprehensive analysis of technical capabilities and performance characteristics, detailed spectrum sharing considerations across multiple frequency bands, extensive future spectrum allocation needs and regulatory implications, and comprehensive future private 6G developments including technological roadmaps and potential applications. Their work provides detailed technical analysis of emerging technologies and their integration with private networks. However, their survey does not cover detailed industrial use cases, specific architecture deployment models (SA/NSA), private 4G/LTE legacy system considerations, or comprehensive device ecosystem coverage for private 5G networks.

Scalise et al. [43] primarily discuss the identity management and security architecture of private 5G networks with detailed analysis of authentication mechanisms and privacy protection protocols, while providing some consideration of future 6G developments from a security and identity perspective. Their work focuses on user identity protection, access control mechanisms, and security framework development. However, their survey does not cover detailed industrial and enterprise use cases, comprehensive spectrum sharing mechanisms, future spectrum allocation demands and regulatory considerations, private 4G/LTE legacy system integration, or device-level compatibility aspects related to private 5G network deployments.

Comparative Analysis of Existing Survey Literature

Our comprehensive analysis of existing survey papers reveals significant gaps in the current literature that our work addresses. The comparative evaluation demonstrates that while several surveys focus on specific aspects of private networks, none provides the holistic coverage that enterprises and researchers require for complete understanding and implementation guidance. Eswaran and Honnavalli's work, while thorough in private 5G coverage, completely omits private 4G/LTE implementations, which remain crucial for many industrial deployments seeking gradual migration paths. Similarly, their limited treatment of use cases and absence of device-specific discussions creates gaps for practitioners seeking concrete implementation guidance.

The analysis reveals a concerning trend where most existing surveys treat spectrum sharing as a secondary consideration rather than a fundamental enabler of private networks. Wang and Jain's work exemplifies this limitation, providing only brief mentions of spectrum sharing without exploring its critical role in making private networks economically viable. This oversight is particularly significant given that spectrum availability and sharing mechanisms directly impact deployment feasibility and operational costs. Furthermore, the absence of future spectrum needs discussion in most surveys limits their utility for strategic planning and long-term investment decisions.

Most notably, the literature demonstrates a clear bias toward current technologies, with limited vision for future developments. Only two surveys (Maman et al. and Patwary et al.) address future private 6G developments, and even these provide limited depth. This represents a critical gap for organizations seeking to make technology investments that will remain relevant over extended deployment lifespans. The lack of comprehensive device ecosystem coverage across all surveys also limits practical implementation guidance, as device availability and compatibility significantly impact deployment success.

Our survey distinguishes itself by providing the only comprehensive treatment spanning all critical dimensions: private 4G/LTE foundations, detailed private 5G implementations, extensive use case analysis, comprehensive spectrum sharing mechanisms, architectural models comparison, future spectrum requirements, device ecosystem coverage, and forward-looking private 6G developments. This holistic approach enables readers to understand not just individual technologies, but their interrelationships and evolution paths, providing essential guidance for both immediate implementation decisions and strategic technology planning.

3. Global spectrum allocations for private 5G deployments

As private 5G networks become increasingly vital for supporting advanced applications across various industries, understanding the spectrum allocations and regulatory frameworks of different countries is essential. These allocations define the frequency bands, maximum spectrum allocations, lease durations, and power limits, which collectively influence the deployment and performance of private 5G networks. Table 3 provides a comprehensive overview of spectrum allocations and transmit power limits for private 5G deployments across several countries. This table highlights the availability of private 5G (P5G) spectrum, the specific frequency bands, frequency ranges, maximum spectrum allocation per enterprise, lease durations, and the maximum indoor radiated power allowed.

3.1. Spectrum sharing models

Spectrum sharing optimizes frequency use in modern telecommunications, exemplified by the CBRS framework in the United States. This dynamic three-tiered model includes Incumbent Access, PAL, and GAA users. Incumbent Access is reserved for primary users (e.g., military and government systems) that retain uninterrupted access. PAL is licensed access, awarded through an auction process, which provides prioritized spectrum availability with specific usage rules. GAA enables unlicensed, opportunistic access when the spectrum is not occupied by either incumbents or PAL users. Several studies have been conducted to analyze different aspects of spectrum sharing within this framework. Tusha et al. present a real-world CBRS deployment analysis that focuses on co-channel interference (CCI) and adjacent channel interference (ACI) in a commercial network. Their study highlights that the Spectrum Access System (SAS) does not manage interference for GAA users effectively, emphasizing the need for dynamic channel selection [44].

Gao and Sahoo (2019) investigated the performance of a GAA coexistence scheme in the CBRS band, focusing on minimizing mutual interference among GAA users while ensuring high spectrum utilization. Their study evaluated one of the Wireless Innovation Forum's recommended coexistence schemes using actual terrain and land cover data in the USA [45]. Jai et al. (2021) developed a mathematical framework for optimal channel allocation in the CBRS band, addressing the coexistence of PAL holders, GAA users, and shipborne radar incumbents with real-world data from Virginia's east coast to ensure both interference protection and efficient spectrum utilization [46]. Berry et al. (2023) review the CBRS framework and evaluate its technical and economic impacts, demonstrating the advantages of dynamic spectrum sharing in reducing costs and delays in commercial spectrum allocation [47]. Agarwal et al. (2022) provide a comprehensive survey on CBRS, detailing its hierarchical architecture, regulatory and standardization process, and industrial developments; they also discuss optimal spectrum sharing and resource allocation schemes while identifying open research issues [48]. Ghosh and Berry (2020) explore the entry and investment decisions of spectrum access firms using a game-theoretic model that examines PAL bidding and investment levels, illustrating how licensed spectrum availability influences market competition [49]. Kang, Balachandran, and Buchmayer (2018) investigate the coexistence performance of GAA use cases with LTE-TDD technologies by evaluating channel allocation solutions managed by a Coexistence Manager (CxM) in a 3D city environment. Their study highlights a trade-off between conservative frequency reuse in indoor Pico networks and increased capacity in outdoor Micro networks [50]. Further, Gao and Sahoo (2020) analyze the performance impact of Coexistence Groups (CxGs) in a GAA–GAA coexistence scheme within the CBRS band using real terrain data, providing insights into interference management and operational efficiency [51]. Gao, Sahoo, and Bradford (2020) evaluate an alternative coexistence approach (Approach 3) for GAA users, offering insights into how to minimize mutual interference and enhance spectrum utilization [52].

Hikmaturokhman et al. (2022) propose a novel formula for calculating spectrum usage fees for 5G-mmWave private networks in Indonesian industrial areas, adopting the ITU-R SM.2012-5 framework and incorporating the Indonesia Industry Readiness Index 4.0 to support cost-effective deployment [53]. Guo et al. (2022) discuss the design of customized 5G and beyond private networks (C5GBPN) for industrial verticals, proposing a flexible paradigm that integrates ultra-reliable low-latency communications (URLLC), enhanced mobile broadband (eMBB), Massive Machine Type Communications (mMTC), and positioning services to overcome limitations of public networks [54]. Bajracharya, Shrestha, and Jung (2020) examine the utilization of unlicensed spectrum via NR-U to support Industry 4.0 applications, addressing regulatory challenges and proposing solutions such as shared maximum channel occupancy time (MCOT) and self-organized networks (SON) to enhance reliability and performance [55]. Chakraborty and Rao (2024) analyze the temporal and spatial behavior of the SAS using a Markov chain model, revealing complexities in spectrum availability reporting and proposing strategies to enhance entropy [56]. Rachakonda et al. (2024) provide a comprehensive study on privacy and security challenges in IoT with a focus on spectrum sharing in next-generation networks, highlighting the benefits and drawbacks of various spectrum-sharing technologies and proposing directions for future research [57]. For another perspective, V. Sathya et al. (2024) analyze battery efficiency in Wi-Fi, CBRS, and macro networks, finding that CBRS-based 5G LAN systems have lower battery consumption due to interference-free channels and efficient resource allocation [58]. Sathya et al. also present a comparative study of WLAN and 5G LAN (CBRS) systems for enterprise applications, demonstrating superior performance of 5G LAN in latency, packet drop, and throughput under high load conditions [59]. Their further analyses of dense warehouse deployments [60] and roaming performance [61] emphasize the advantages of CBRS in supporting robust 5G private networks.

Table 2 summarizes the key studies discussed above, outlining their focus areas, methodologies, and contributions toward understanding the efficacy of spectrum sharing models in supporting 5G private networks.

Comprehensive Analysis of Spectrum Sharing Research Landscape

The systematic analysis of spectrum sharing studies reveals a mature research ecosystem with distinct focus areas that collectively demonstrate the viability and complexity of dynamic spectrum access in private networks. Performance-focused studies (Tusha et al. Gao and Sahoo, Kang et al.) consistently reveal that while CBRS framework enables successful spectrum sharing, significant challenges remain in interference management, particularly for GAA users who lack dedicated protection mechanisms. These findings indicate that current SAS implementations require enhancement to provide more sophisticated interference coordination, suggesting that pure market-based spectrum sharing has limitations that necessitate more intelligent coordination mechanisms.

Economic and regulatory studies (Berry et al. Ghosh and Berry, Agarwal et al.) demonstrate compelling evidence that dynamic spectrum sharing reduces both deployment costs and regulatory complexity compared to traditional exclusive licensing approaches. The CBRS framework's success in generating substantial auction revenues ($4.6 billion in PAL auctions) while simultaneously enabling GAA access proves that shared spectrum models can satisfy both government revenue requirements and commercial deployment needs. However, the investment behavior analysis reveals that PAL holders often underutilize acquired spectrum, suggesting that auction mechanisms may need refinement to ensure efficient spectrum utilization rather than speculative holding.

Technical implementation studies (Jai et al. Gao et al. Hikmaturokhman et al.) reveal that successful spectrum sharing requires sophisticated mathematical frameworks and real-world environmental considerations that significantly impact performance. The geographic and

Table 2
Summary of spectrum sharing studies with detailed analysis [44–61].

Study	Focus/Methodology	Key findings and relevance	Limitations and gaps
Tusha et al. [44]	Real-world CBRS deployment analysis	Identified CCI and ACI issues for GAA users; highlighted SAS limitations in managing interference.	Limited to single geographical area; lacks multi-vendor equipment testing; no long-term performance analysis.
Gao and Sahoo (2019) [45]	GAA coexistence scheme using terrain data	Minimized mutual interference among GAA users and optimized bandwidth allocation.	Simulation-based study; limited real-world validation; focuses only on GAA tier interactions.
Jai et al. (2021) [46]	Mathematical framework for channel allocation	Ensured interference protection and efficient spectrum utilization among PAL, GAA, and incumbents.	Theoretical model lacks practical implementation details; limited to specific geographic region; no economic analysis.
Berry et al. (2023) [47]	Review of the CBRS three-tier model	Assessed technical and economic impacts; demonstrated benefits of dynamic spectrum sharing.	Review paper with limited original research; lacks detailed technical implementation guidance; US-centric perspective.
Agarwal et al. (2022) [48]	Comprehensive survey on CBRS	Detailed CBRS architecture, regulatory process, and resource allocation; identified open research areas.	Survey format limits practical insights; insufficient coverage of global spectrum sharing models; lacks performance benchmarks.
Ghosh and Berry (2020) [49]	Game-theoretic analysis of PAL bidding	Illustrated the impact of licensed spectrum on market competition.	Theoretical economic model; limited real-world market validation; focuses only on PAL tier economics.
Kang et al. (2018) [50]	Evaluation of LTE-TDD based coexistence	Discussed trade-offs between conservative frequency reuse and network capacity.	Limited to LTE-TDD technology; simulation-based results; lacks comprehensive interference mitigation strategies.
Gao and Sahoo (2020) [51]	Performance analysis of Coexistence Groups (CxGs)	Provided metrics for interference management and operational efficiency in GAA schemes.	Focuses only on CxG mechanisms; limited scalability analysis; lacks multi-technology coexistence evaluation.
Gao, Sahoo, and Bradford (2020) [52]	Evaluation of an alternative GAA coexistence approach (Approach 3)	Offered insights into minimizing mutual interference and enhancing spectrum utilization.	Limited to single coexistence approach; lacks comparative analysis with other methods; simulation-based validation only.
Hikmaturokhman et al. (2022) [53]	Spectrum fee calculation model	Proposed a novel fee formula that supports cost reduction for 5G-mmWave deployments.	Country-specific model; limited applicability to other regulatory frameworks; lacks market adoption validation.
Guo et al. (2022) [54]	Design of customized private networks	Proposed integration of URLLC, eMBB, mMTC, and positioning for industrial applications.	Conceptual framework lacks implementation details; limited spectrum efficiency analysis; no cost-benefit evaluation.
Bajracharya, Shrestha, and Jung (2020) [55]	Analysis of NR-U in unlicensed spectrum	Addressed regulatory challenges and proposed solutions (MCOT and SON) for Industry 4.0.	Limited to unlicensed spectrum only; lacks comprehensive interference analysis; theoretical solutions without validation.
Chakraborty and Rao (2024) [56]	Temporal and spatial analysis of SAS using a Markov chain model	Revealed complexities in spectrum availability reporting; proposed strategies for enhanced entropy.	Mathematical model lacks practical implementation; limited to SAS behavior analysis; no end-user impact assessment.
Rachakonda et al. (2024) [57]	Study on privacy and security in IoT with spectrum sharing	Highlighted the benefits of efficient spectrum utilization and proposed future security research.	Security-focused with limited spectrum efficiency analysis; lacks practical deployment guidelines; theoretical security framework.
V. Sathya et al. (2024) [58]	Analysis of battery efficiency in Wi-Fi, CBRS, and macro networks	Found lower battery consumption in CBRS-based 5G LAN systems compared to Wi-Fi.	Limited device types tested; specific use case scenarios; lacks large-scale deployment validation.
Sathya et al. (Commercial Study) [59]	Comparative study of WLAN and 5G LAN systems	Demonstrated superior performance of 5G LAN in latency, packet drop, and throughput under high load.	Limited to enterprise environments; specific vendor equipment; lacks cost comparison analysis.
Sathya et al. (Warehouse Deployment) [60]	Performance analysis in dense warehouse settings	Showed that CBRS maintained low packet drops and latency, outperforming Wi-Fi in dynamic conditions.	Single environment testing; limited mobility scenarios; lacks interference from external sources analysis.
Sathya et al. (Roaming Performance) [61]	Analysis of roaming between Wi-Fi and private networks	Emphasized challenges in Wi-Fi roaming and the benefits of CBRS for improved service continuity.	Limited roaming scenarios tested; specific device types; lacks seamless handover mechanism evaluation.

environmental specificity of interference patterns means that spectrum sharing solutions cannot rely on generic models but must incorporate detailed terrain data, building characteristics, and usage patterns. This finding has profound implications for global spectrum sharing adoption, as each regulatory environment will require customized technical frameworks rather than simple replication of CBRS models.

Table 3
Spectrum allocations and transmit power limits for private 5G deployments in several countries [62].

Country	P5G spectrum available?	Freq band	Freq range [MHz]	Max spectrum allocation per enterprise	Max lease duration [years]	Max indoor radiated power [dBm]	Spectrum management organization	Spectrum sharing techniques
USA	Yes	N48	3550–3700	150 MHz	None	30 dBm	FCC, SAS providers	Dynamic Spectrum Sharing (DSS, CBRS)
Mexico	Yes	N78	3550–3600	50 MHz	TBD	30 dBm [TBC]	IFT, MNOs	DSS
Brazil	Yes	N78	3700–3800	100 MHz	TBD	30 dBm	ANATEL	DSS
Belgium	Yes	N77	3800–4200	40 MHz	TBD	30 dBm	BIPT	Shared access
Netherlands	Yes	N78	3400–3450 & 3750–3800	50 MHz + 50 MHz	Until 2040	31 dB μV/m/5 MHz at 3 m height	RDI	DSS
Ireland	Yes	N77	TBD	TBD	TBD	TBD	ComReg	Shared access
Germany	Yes	N78	3700–3800	100 MHz	10 years	32 dB μV/m/5 MHz at 3 m height	BNetzA	DSS
Switzerland	Yes	N78	3400–3500	100 MHz	TBD	TBD	BAKOM/ OFCOM	Shared access
China	Yes	N78	3300–3400	100 MHz	TBD	TBD	MIIT, MNOs	Spectrum sharing with incumbents
Japan	Yes	N79	4600–4900	300 MHz	15 years	27 dBm	Soumu	Local licensing
South Korea	Yes	N78	3420–3700	280 MHz	10 years	30 dBm	Ministry of Science and ICT	DSS
Turkey	Yes	N78	3300–3800	100 MHz	10 years	30 dBm	ICTA	Spectrum sharing with incumbents
Australia	Yes	N78	3300–3800	100 MHz	10–20 years	30 dBm	ACMA	Leased spectrum
France	Yes	N78	3300–3800	100 MHz	10–15 years	30 dBm	ARCEP	Leased spectrum
Canada	Yes	N78	3300–3800	200 MHz	20 years	30 dBm	ISED	Spectrum sharing with incumbents

Industrial application studies (Guo et al. Bajracharya et al. Sathya et al.) provide compelling evidence that spectrum sharing enables private network deployments that would otherwise be economically unfeasible, particularly for industrial IoT and specialized applications. The battery life and performance comparisons consistently favor CBRS-based private networks over Wi-Fi alternatives, primarily due to interference-free operation and efficient resource allocation. However, these studies also reveal that deployment success heavily depends on proper network planning and integration with existing industrial systems, suggesting that spectrum sharing technology requires significant implementation expertise to realize its full potential.

The following subsections examine the specifics for each country listed.

3.2. North America

Spectrum sharing is a regulatory approach that allows multiple users to access the same frequency band under defined conditions, thereby maximizing spectrum efficiency. Unlike traditional exclusive spectrum allocations, it enables different users to share portions of the band as long as they adhere to the rights and priorities of primary users. This approach is particularly effective in bands where critical services – such as military radar and defense communications – operate intermittently, leaving spectral resources underutilized. In turn, secondary users may access these frequencies when primary users are inactive, optimizing the overall utilization of valuable spectrum.

In the United States, the FCC implemented spectrum sharing in the 3.5 GHz band through the CBRS framework. The 3.5 GHz mid-band, often called the “sweet spot” for wireless communications due to its optimal balance between coverage and capacity, is heavily used by government entities. To enhance its commercial potential, the CBRS initiative divides the 3.5 GHz band into three tiers – Incumbent Access, PAL, and GAA – each governed by specific usage rules [63] (see Fig. 2).

Within this framework:

- **Tier 1 (Incumbent Access):** Reserved for primary users, principally the U.S. Department of Defense and other government entities, ensuring uninterrupted operation of critical services.
- **Tier 2 (Priority Access License, PAL):** Provides licensed, secondary access obtained through auction. PAL holders enjoy priority over unlicensed users but must yield to Tier 1 incumbents as needed.
- **Tier 3 (General Authorized Access, GAA):** Offers opportunistic, unlicensed access to the remaining spectrum, suited for applications such as Wi-Fi offloading, IoT connectivity, and private LTE deployments, with GAA users deferring to both incumbent and PAL users.

In the USA, private 5G spectrum is available in the N48 band (3550–3700 MHz) under the CBRS framework, allowing up to 150 MHz of spectrum with no fixed maximum lease duration. The FCC oversees this framework, which uses SAS providers to dynamically assign spectrum and prevent interference. The maximum indoor radiated power is 30 dBm, supporting robust network performance in various environments [63–65]. Mexico offers private 5G spectrum in the N78 band (3550–3600 MHz), with up to 50 MHz accessible for enterprises. The Federal Telecommunications Institute (IFT) and MNOs manage spectrum allocation, employing Dynamic Spectrum Sharing (DSS) techniques. The maximum indoor radiated power is 30 dBm, enhancing signal penetration within indoor settings [66,67]. Canada provides private 5G spectrum in the N78 band (3300–3800 MHz), with up to 200 MHz available for 20 years. Innovation, Science and Economic Development Canada (ISED) oversees spectrum allocation, using spectrum sharing with incumbents. The maximum indoor radiated power is 30 dBm [62,68].

3.3. South America

In Brazil, private 5G spectrum is available in the N78 band (3700–3800 MHz), with up to 100 MHz accessible for enterprises. ANATEL oversees spectrum allocation and employs DSS techniques. The maximum indoor radiated power is 30 dBm, ensuring effective indoor coverage [69,70].

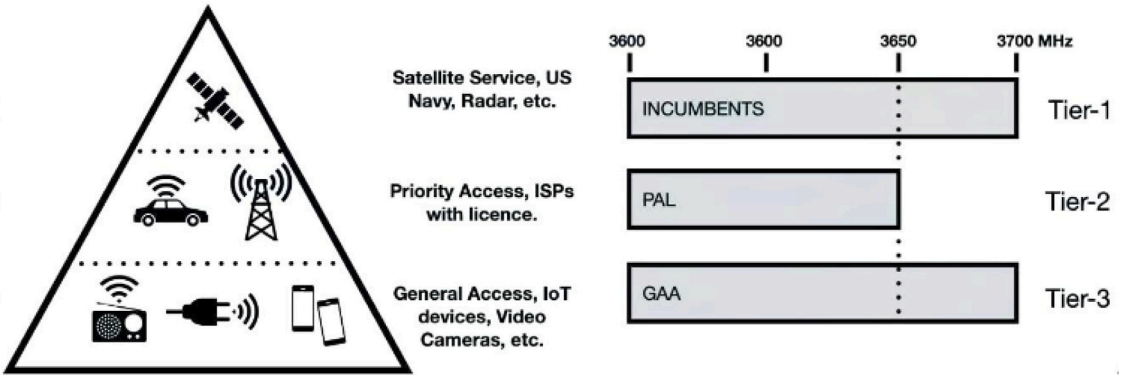

Fig. 2. The Three-Tier CBRS Architecture: This diagram illustrates the CBRS framework, divided into Incumbents, PALs, and GAA, each with distinct levels of access and protection for efficient use of the 3550–3700 MHz band.

3.4. Europe

Belgium provides private 5G spectrum in the N77 band (3800–4200 MHz), with up to 40 MHz accessible for enterprises. Belgian Institute for Postal Services (BIPT) manages spectrum allocation, utilizing Shared Access techniques. The maximum indoor radiated power is 30 dBm, supporting various high-performance applications [71,72]. The Netherlands offers private 5G spectrum in the N78 band (3400–3450 MHz and 3750–3800 MHz), with two 50 MHz blocks available until 2040. RDI oversees spectrum allocation, using DSS techniques. The maximum indoor radiated power is 31dB μV/m/5 MHz at 3 m height [73,74]. In Ireland, private 5G spectrum in the N77 band is available, but specific details are still TBD. ComReg oversees spectrum allocation, likely employing Shared Access techniques [75–77]. Germany provides private 5G spectrum in the N78 band (3700–3800 MHz), with up to 100 MHz available for 10 years. Bundesnetzagentur (BNetzA) manages spectrum allocation, employing DSS techniques. The maximum indoor radiated power is 32dB μV/m/5 MHz at 3 m height [78–80]. Switzerland offers private 5G spectrum in the N78 band (3400–3500 MHz), with up to 100 MHz accessible. Federal Office of Communications (BAKOM/OFCOM) oversees spectrum allocation, using Shared Access techniques. Specific lease duration and power limits are TBD [81–83]. France offers private 5G spectrum in the N78 band (3300–3800 MHz), with up to 100 MHz available for 10–15 years. France's Regulatory Authority for Electronic Communications, Postal Affairs and Press Distribution (ARCEP) oversees spectrum allocation, using leased spectrum techniques. The maximum indoor radiated power is 30 dBm [62,84].

3.5. Asia

China's private 5G spectrum in the N78 band (3300–3400 MHz) allows up to 100 MHz for enterprises. Ministry of Industry and Information Technology (MIIT) and MNOs manage allocation, using spectrum sharing with incumbents. Lease duration and power limits are TBD [85–87]. Japan offers private 5G spectrum in the N79 band (4600–4900 MHz), with up to 300 MHz available for 15 years. Soumu manages spectrum allocation, using local licensing techniques. The maximum indoor radiated power is 27 dBm [88–90]. South Korea provides private 5G spectrum in the N78 band (3420–3700 MHz), with up to 280 MHz available for 10 years. The Ministry of Science and ICT manages allocation, using DSS techniques. The maximum indoor radiated power is 30 dBm [91–93]. Turkey offers private 5G spectrum in the N78 band (3300–3800 MHz), with up to 100 MHz available for 10 years. ICTA oversees spectrum allocation, using spectrum sharing with incumbents. The maximum indoor radiated power is 30 dBm [62].

3.6. Australia

Australia provides private 5G spectrum in the N78 band (3300–3800 MHz), with up to 100 MHz available for 10–20 years. Australian Communications and Media Authority (ACMA) manages spectrum allocation, using leased spectrum techniques. The maximum indoor radiated power is 30 dBm [62,94].

// Add this new subsection in Section 3

3.7. Alternative spectrum access methods for private networks

In countries where all spectrum is allocated to operators' public networks and dedicated private spectrum is unavailable, organizations must explore alternative approaches to deploy private networks. These alternatives include operator collaboration models and unlicensed spectrum solutions that can provide cost-effective private network deployment options.

Operator Collaboration Models: When dedicated spectrum is unavailable, private network deployment requires negotiation with mobile network operators (MNOs) for spectrum sharing arrangements or network slicing services. This collaborative approach enables enterprises to access cellular spectrum through service agreements with operators, though it inherently involves operational costs and dependency on operator infrastructure.

License Assisted Access (LAA) Solutions: LAA technology enables LTE networks to utilize unlicensed 5 GHz spectrum alongside licensed spectrum, providing additional capacity for private network deployments. LAA employs listen-before-talk (LBT) mechanisms to coexist with Wi-Fi and other unlicensed users, making it a viable option for private networks in spectrum-constrained environments [95,96].

NR-Unlicensed (NR-U) Technology: NR-U extends 5G New Radio capabilities to unlicensed spectrum bands, including 5 GHz and 6 GHz frequencies. This technology allows private 5G networks to leverage unlicensed spectrum while maintaining 5G performance characteristics, providing enterprises with deployment flexibility without requiring licensed spectrum allocations [97,98].

These alternative approaches offer practical solutions for private network deployment in regulatory environments where dedicated spectrum allocation is not available. While the ideal solution remains dedicated spectrum allocation, LAA and NR-U technologies provide viable pathways for cost-conscious deployments that can adapt to any country's regulatory framework [99–101].

4. Architectures for private deployment

First, we review several studies that explore various aspects of network architectures in private 5G deployments, including performance enhancements, resource allocation strategies, and security measures. Then, we explain the three main architectures used in private

deployments – 4G, non-standalone, and completely standalone 5G – highlighting that each offers distinct benefits and is tailored for specific deployment scenarios.

4.1. Network architectures in private deployments

Luo et al. (2021) investigate the design and performance of in-band full-duplex (IBFD) private 5G networks in the FR2 band (≤24.250 GHz). Their work emphasizes the use of large-scale antenna arrays, RF beamforming, and self-interference cancellation (SIC) schemes to support URLLC and URLLCeMBB simultaneously. They also introduce a game-theoretic user allocation algorithm to minimize co-channel interference (CCI), demonstrating significant improvements in bit error rate (BER) and spectral efficiency (SE).

The document by Braun et al. details an architecture for building and managing Quality of Service (QoS)-enabled virtual private networks (VPNs) over the Internet. It introduces the fundamental technologies necessary for secure VPNs with QoS support, explains the vision of a QoS-enabled VPN service, and provides an implementation scenario for achieving both security and QoS.

Homayouni et al. (2023) explore the practical realization of a private 5G standalone network tailored for vertical industries, with a special focus on smart factory applications. Their study provides a comprehensive overview of the conceptual architecture, deployment, and operational demonstrations, including key performance metrics such as uplink/downlink performance and round-trip-time delay. Additionally, another work by Homayouni et al. (2023) evaluates the 3GPP Release 16 specifications for indoor positioning within a private 5G network in smart factory environments, showing positioning accuracy ranging from less than a meter up to a few meters.

Turchet and Casari (2023) assess the capability of private 5G standalone (SA) versus public 5G non-standalone (NSA) architectures to support Networked Music Performances (NMPs). Their analysis of network metrics – including end-to-end latency and packet error ratio – demonstrates that the private 5G SA network, with edge computing integration, meets the stringent latency and reliability requirements needed for realistic music interplay.

John et al. (2022) describe a reference deployment of a minimal open-source private 5G SA system for industry and campus environments. Their work underscores deployment challenges associated with open-source implementations, highlighting a cost-effective solution that achieves basic connectivity alongside measurable latency and throughput.

Arpitha and Anand (2022) design, dimension, and test a 5G Core (5GC) network using SDN-NFV technologies for services such as Industrial internet of things (IIoT),MCS (Modulation and Coding Scheme), C-V2X (Cellular Vehicle-to-Everything) and VoNR (Voice over New Radio). Their study addresses capacity and functional requirements for industrial sectors like oil and gas, and demonstrates efficient handling of significant user and device loads.

Vosteen et al. (2022) perform a security analysis for private 5G industrial SA deployments by using off-the-shelf components and open-source software. They identify potential attack vectors and propose measures to improve network security through additional testing. Complementarily, Tripathi, Thakur, and Tamma (2022) analyze insider attacks on standalone non-public 5G networks using attack graphs and offer recommendations for strengthening security controls.

4.2. 4G architecture

Private 4G networks, commonly referred to as private LTE, provide a dedicated and isolated network infrastructure that operates independently of public cellular networks. This architecture is ideally suited for environments that require high reliability, low latency, and secure communications, such as manufacturing, logistics, and public safety [102,103]. In these deployments, the network is designed and optimized to meet the specific operational demands of an enterprise.

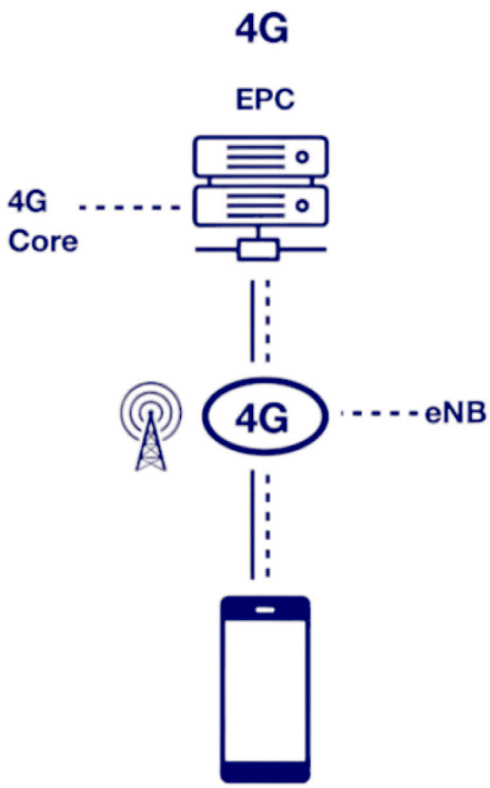

Fig. 3. Private 4G network architecture.

The private 4G architecture comprises several key components, as illustrated in Fig. 3:

- **4G Core (EPC):** The EPC is the central component of the 4G LTE system and is responsible for user authentication, mobility management, and data routing. Its centralized architecture ensures efficient handling of both signaling and data, which is vital for maintaining network reliability [104].
- **Base Stations (eNodeBs or eNBs):** These radio access points are deployed strategically to ensure robust coverage and sufficient capacity. Optimal placement of eNodeBs is critical, especially in industrial settings where physical obstructions and interference can affect signal quality.
- **User Equipment (UE):** Devices such as smartphones, tablets, and specialized IoT devices (including industrial sensors and automated guided vehicles) rely on the network to perform critical communication functions [102].
- **Backhaul Network:** This component connects the eNodeBs to the EPC, ensuring reliable data transmission across the network. Backhaul can be implemented via wired or wireless methods, and its performance directly influences the overall network throughput and latency.
- **Network Management System (NMS):** The NMS monitors, manages, and optimizes network performance, ensuring that all components operate in harmony and that deployment-specific requirements are consistently met [103].

Despite its advantages, the private 4G architecture exhibits several significant limitations that hinder its suitability for modern industrial deployments. One of the primary constraints is its limited scalability, which stems from the inherent spectral efficiency of 4G technology. The modulation schemes and coding techniques employed in 4G, although

effective under moderate conditions, are not designed to handle the high-density, data-intensive requirements of today's enterprise environments. This limitation is compounded by the reliance on legacy protocols that lack the advanced features needed to support dynamic network slicing and adaptive resource management.

Moreover, the overall performance of 4G networks in terms of data rates and latency is inadequate for many contemporary applications. In industrial settings where machine-critical processes depend on rapid data exchange and immediate response times, even slight delays can lead to substantial inefficiencies or operational risks. The typical throughput and latency metrics of 4G are often insufficient for applications that demand ultra-low latency and high throughput, such as real-time control systems and automated production lines.

Furthermore, as the number of IoT devices increases and data consumption continues to surge, 4G networks face growing challenges in future-proofing their infrastructure. The legacy design of 4G does not easily accommodate the massive connectivity and higher performance requirements projected for the near future. These factors collectively make it challenging for 4G networks to sustain the evolving demands of modern industries [102–104].

4.3. NSA 5G architecture

The NSA 5G architecture enables early deployment of 5G services by leveraging an existing 4G LTE infrastructure. In NSA, the 5G New Radio (NR) is integrated with the 4G Evolved Packet Core (EPC), where the control plane continues to operate through the 4G core, while the user plane can utilize 5G radio capabilities. This configuration supports higher throughput and lower latency than pure 4G, offering a practical step toward full 5G deployment [105].

NSA is widely adopted by MNOs seeking rapid rollout of 5G without waiting for full 5G Core (5GC) readiness. Major carriers such as Verizon and AT&T have used NSA architecture to introduce 5G coverage by building upon their established 4G networks [106]. This hybrid setup minimizes deployment cost and time while extending 5G availability.

While NSA is typically associated with public networks, it can also be employed in private network scenarios. A key clarification is that NSA does not necessarily require reliance on public MNO infrastructure. A private 4G core – deployed and managed independently – can serve as the control plane anchor for NSA in private settings such as industrial campuses, warehouses, or ports. In these cases, NSA may offer a viable architecture for organizations that already operate a private LTE system and are looking to enhance performance through 5G NR [105].

However, NSA may introduce complexity in achieving certain 5G-native features like ultra-low latency and network slicing, which are fully supported in SA architecture. Thus, while NSA is feasible for private deployments, organizations aiming for the most advanced 5G capabilities and flexibility may still prefer SA architecture.

4.4. Completely standalone 5G architecture

Standalone 5G (SA 5G) networks leverage the 5G New Radio (NR) and a dedicated 5G Core (5GC) to operate independently of legacy 4G infrastructure. This architecture is engineered to deliver significantly enhanced performance, flexibility, and a wider range of capabilities, making it particularly well-suited for private deployments that require high performance and scalability. SA 5G networks are capable of supporting ultra-reliable low latency communications (URLLC), massive machine-type communications (mMTC), and URLLCeMBB, which are all critical for addressing the complex demands of industrial and mission-critical applications [107,108] (see Fig. 4).

The SA 5G architecture comprises several essential components that work together to deliver high performance:

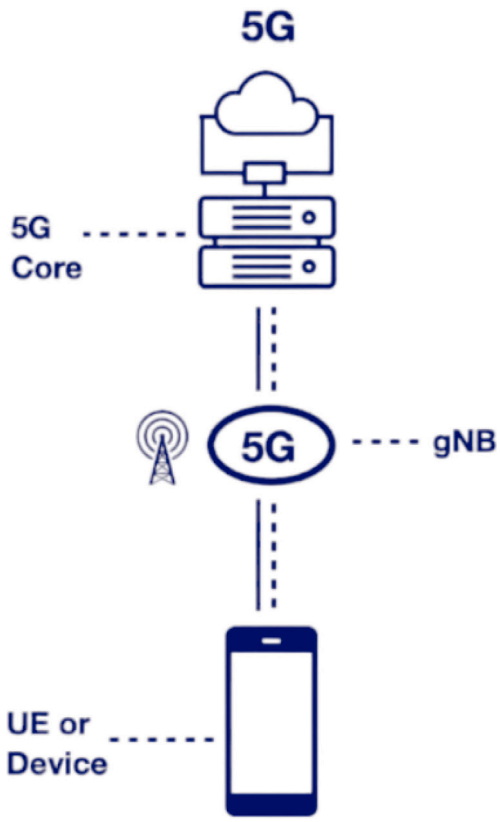

Fig. 4. Private 5G network architecture.

- **5G Core (5GC):** Serving as the backbone of the network, the 5GC handles tasks such as user authentication, mobility management, and data routing with a design optimized for high throughput and very low latency [107].
- **Base Stations (gNodeBs or gNBs):** These advanced radio access points are strategically deployed to ensure optimal coverage and capacity. In private 5G settings, the careful placement and configuration of gNBs are crucial for achieving a consistent and high-quality connection across the deployment area [108].
- **User Equipment (UE):** This includes smartphones, tablets, and a range of IoT devices that connect to the network. These devices are designed to take full advantage of the enhanced features and lower latency offered by SA 5G [109].
- **Backhaul Network:** The backhaul is responsible for connecting the gNBs to the 5GC, thereby supporting the high data rates and low latency requirements of 5G. Both wired and wireless backhaul options are utilized depending on the specific deployment context [110].
- **Network Management System (NMS):** An integral component that monitors and optimizes the network's performance, the NMS ensures that the deployment adapts to changes in demand and maintains service quality in line with the deployment's requirements [111].

The benefits of the completely standalone 5G architecture are substantial and multifaceted. SA 5G offers markedly enhanced performance by delivering significantly higher data rates and drastically lower latency than both private 4G and NSA 5G networks. This performance improvement is achieved through the use of a dedicated 5G core (5GC) that eliminates the bottlenecks inherent in legacy 4G systems, ensuring that even the most data-intensive and latency-sensitive applications – such as autonomous control systems, real-time industrial automation,

Table 4
Comparison of 4G and 5G SA in private networks.

Feature	Private 4G (LTE)	Private 5G Standalone (SA)
Throughput	Moderate (up to 100 Mbps typical)	High (1 Gbps or more depending on deployment)
Latency	30–50 ms (RTT)	As low as 1 ms (with URLLC and edge computing)
URLLC support	Not supported natively	Fully supported with 5G Core
mMTC (massive IoT)	Limited support	Full support (scalable connectivity)
eMBB (Enhanced Mobile Broadband)	Basic broadband for mobile devices	High-speed broadband for bandwidth-intensive apps
Network slicing	Not supported	Fully supported with flexible, dedicated slices
Edge computing integration	Limited and external	Natively supported and optimized
Scalability	Moderate (suitable for small/medium sites)	High (suitable for large-scale industrial IoT)
Security	Based on LTE security architecture	Advanced 5G-native security with dedicated core

and mission-critical IoT services – operate reliably and with minimal delay [112].

Furthermore, the flexibility inherent in SA 5G allows for highly customized network deployments that can be fine-tuned to meet specific industrial or enterprise requirements. This adaptability is crucial in environments where network demands can vary widely between different applications, locations, or operational scenarios, enabling operators to allocate resources dynamically and optimize network performance based on real-time needs [113].

SA 5G also supports advanced capabilities such as ultra-reliable low latency communications (URLLC), massive machine-type communications (mMTC), and URLLCeMBB. These features collectively provide a robust framework that supports a broad spectrum of mission-critical applications, ranging from high-definition video streaming and virtual reality to real-time control systems in smart factories. This capacity to support diverse applications with stringent performance requirements sets SA 5G apart from earlier network architectures.

In addition to performance benefits, the dedicated nature of the 5G core in SA 5G leads to improved security. With a standalone core designed specifically for 5G, enhanced security protocols and measures are more effectively integrated, ensuring that sensitive communications and critical data are better protected against cyber threats [114–116]. Moreover, the architecture is future-proofed, facilitating seamless integration of emerging technologies such as edge computing and AI-driven network management, which further enhance network capabilities and allow for continual technological evolution without necessitating major infrastructure overhauls.

Table 4 provides a comparison between private 4G and 5G Standalone networks in terms of performance, capabilities, and architectural differences.

4.5. Comparison of NSA and SA architectures

Table 5 below provides a detailed comparison of key features between NSA and SA architectures, with additional columns that outline the implications for private network deployments. This table not only contrasts fundamental attributes such as core network design, deployment speed, and coverage areas but also examines essential performance characteristics including data throughput, latency, and overall signal reliability. In addition, it incorporates important factors such as security measures, the level of flexibility and customization available, and the cost implications at both the initial deployment and long-term operational levels. These aspects are critical for evaluating the suitability of a network architecture for private applications, where tailored performance, robust security, and scalability are vital for supporting mission-critical and industrial use cases. The detailed presentation in Table 5 enables a comprehensive evaluation of the trade-offs and benefits associated with NSA versus SA, thereby providing clear guidance for selecting the optimal deployment strategy in private network environments.

4.5.1. Comparing distinct SA deployments for private networks

Beyond the broad comparison between NSA and SA architectures, it is important to consider variations among distinct SA deployments, as different configurations may be better suited to private network scenarios depending on specific requirements. For example, one SA deployment might integrate advanced edge computing capabilities and sophisticated network slicing to isolate mission-critical traffic. This configuration would excel in environments where ultra-low latency and high throughput are paramount, such as manufacturing floors or healthcare facilities where real-time control is critical. In contrast, another SA deployment could be designed to maximize geographic coverage with a distributed architecture and robust backhaul solutions, which might be more beneficial in large campus environments or extensive industrial sites, albeit with a trade-off in extreme latency performance.

When comparing two SA deployments, key factors to evaluate include:

- **Edge Computing Integration:** Deployments featuring localized edge processing can dramatically lower end-to-end latency by processing data near its source.
- **Network Slicing Capabilities:** Advanced slicing provides dedicated virtual networks that prioritize critical applications, enhancing performance consistency.
- **Backhaul Architecture:** The quality and capacity of the backhaul network directly affect throughput and latency; a robust backhaul is essential for high-demand applications.
- **Scalability and Flexibility:** Configurations that are designed for future expansion and can adapt dynamically to increasing device density or application demands are more likely to deliver long-term value in private deployments.

In summary, the SA deployment that best meets the needs of a private network will be the one that offers superior edge computing integration, advanced slicing for resource management, a resilient high-capacity backhaul, and flexible scalability options. The optimal configuration will depend on the specific application requirements and operational environment, ensuring that performance, reliability, and security are maintained at the desired levels for mission-critical tasks.

Table 5
Detailed comparison of NSA and SA architectures for private networks.

Feature	Non-Standalone (NSA)	Standalone (SA)	Implications for private networks
Core network	4G EPC integrated with 5G radio	Dedicated 5G Core (5GC) architecture	SA delivers superior performance and security by eliminating legacy protocol constraints.
Deployment Speed	Rapid deployment leveraging existing 4G infrastructure	Slower, new infrastructure required	NSA may enable faster rollout; however, SA provides a more robust and tailored solution for private environments.
Coverage	Optimized for wide-area, consumer-focused service	Designed for dedicated, localized coverage	SA architecture is better suited for confined enterprise or industrial environments demanding precise coverage.
Performance	Constrained by legacy 4G limitations; moderate data rates and throughput	Full 5G capabilities with high throughput and extremely low latency	SA is critical for mission-critical applications that require real-time data processing.
Latency	Generally higher due to intermediary 4G core processing	Lower latency with end-to-end 5G design	The reduced latency in SA networks is essential for applications such as real-time control and automation.
Security	Limited by legacy security measures inherent in 4G EPC	Enhanced security with 5G-specific protocols and dedicated core functions	SA provides a more secure environment, vital for protecting sensitive industrial operations.
Flexibility & Customization	Less flexible; constrained by existing public network configurations	High degree of customization possible through network slicing and tailored resource allocation	SA allows for bespoke network configurations that can be fine-tuned to meet specific enterprise demands.
Cost	Lower initial costs by leveraging current infrastructure	Higher upfront investment for new network elements	Although NSA has lower initial costs, SA offers a more sustainable and efficient solution for long-term, mission-critical deployments.

5. Advantages of private 5G over MNOs and Wi-Fi

Private 5G networks provide significant advantages over traditional MNOs and Enterprise Wi-Fi, making them a superior choice for modern enterprises. By leveraging coordinated spectrum use, private 5G ensures interference-free, high-capacity connectivity with customizable coverage for large industrial sites. Unlike Wi-Fi, which often suffers from congestion and interference, private 5G offers ultra-low latency (less than 1 ms), enhanced security through dedicated measures, and scalable support for millions of devices. These networks provide deterministic Quality of Service (QoS) through scheduling and RF feedback loop controls, ensuring consistent performance even in high-density environments [38,117]. Furthermore, private 5G supports seamless mobility with precisely timed handovers, ensuring continuous connectivity for moving devices.

While Wi-Fi and MNOs have their specific use cases, they often fall short in meeting the demands of modern enterprises. Wi-Fi is limited to smaller indoor areas, offering moderate security and capacity, while MNOs, although reliable, are shared with public users and controlled by operators. In contrast, private 5G excels in density handling, customization, and control, providing high reliability through guaranteed performance via Service Level Agreements (SLAs) [118]. The moderate initial investment in private 5G leads to lower long-term operational costs, making it a cost-effective solution for mission-critical applications in sectors such as healthcare, manufacturing, and logistics. Table 6 highlights the distinct advantages of private 5G networks over MNOs and Enterprise Wi-Fi.

The table provides a detailed comparison of Private 5G, MNOs, and Enterprise Wi-Fi across various aspects. Private 5G networks use coordinated spectrum managed by SAS for CBRS, offering 150 MHz with centralized protections, while MNOs operate on licensed spectrum managed by operators, and Enterprise Wi-Fi uses unlicensed spectrum, leading to potential interference despite having 563 MHz plus 1.2 GHz in the 6 GHz bands [117,118]. Coverage varies significantly, with Private 5G customizable for large sites and higher transmit power using OFDMA sub-carriers (15 kHz), MNOs providing wide-area coverage with managed interference, and Enterprise Wi-Fi limited to 100 m indoors [38]. Latency is ultra-low for Private 5G at less than 1 ms, making it ideal for real-time applications, while MNOs have moderate latency (30–50 ms) and Wi-Fi ranges from 10–100 ms, often too high for demanding tasks.

In terms of security, Private 5G offers high security with dedicated measures, MNOs provide high security through SIM-based measures but share networks with public users, and Wi-Fi security is moderate, despite improvements with WPA3 encryption [119]. Capacity is highest in Private 5G at up to 10 Gbps, compared to 1–3 Gbps for MNOs and 100–300 Mbps for Wi-Fi. Private 5G also supports millions of devices, ideal for large-scale IoT deployments, whereas MNOs and Wi-Fi are more limited [38]. Control is high in Private 5G, allowing full customization, whereas MNOs offer low control and Wi-Fi is high (enterprise dependent). Reliability is also highest in Private 5G with 99.999% SLAs, compared to 99.99% for MNOs and 99% for Wi-Fi [38].

Private 5G offers high customization tailored to specific enterprise needs, enhancing operational efficiency and supporting specialized applications [117]. It is designed for industry-specific, mission-critical applications, supporting advanced use cases in automation, smart cities, and telemedicine. Wi-Fi is more suitable for home and small business environments, while MNOs cater to general public use. In terms of cost, Wi-Fi equipment is inexpensive but lacks scalability, MNOs have high operational costs, and Private 5G, with a moderate initial investment, offers lower long-term costs through TCO savings, making it cost-effective for enterprises.

Traffic handling in Private 5G is managed by scheduling through infrastructure with weighted profiles, while MNOs handle traffic with prioritized management and Wi-Fi relies on distributed contention, leading to inefficiencies [117]. Quality of Service (QoS) is deterministic in Private 5G with mandatory RF feedback controls, high in MNOs with SLAs, and statistically prioritized in Wi-Fi, leading to variable performance. Private 5G supports high-density environments with dual-factor OFDMA and non-blocking interference, MNOs optimize for urban density, and Wi-Fi suffers from blocking co-channel interference, reducing efficiency in dense settings. Mobility is best supported by Private 5G with precise handovers, followed by MNOs with seamless mobility,

Table 6
Comparison of Private 5G, MNOs, and Enterprise Wi-Fi [117,118].

Feature/Aspect	Private 5G	MNOs	Enterprise Wi-Fi
Spectrum coordination	Coordinated spectrum use by SAS, 150 MHz available, Centralized incumbent protections	Licensed spectrum use, Coordinated by MNOs, high availability	Unlicensed spectrum use, 563 MHz plus 1.2 GHz in 6 GHz bands, Distributed incumbent protection
Coverage	Customizable for large sites, Higher transmit power, OFDMA sub-carriers (15 kHz)	Wide area coverage, High power transmission, Managed interference	Up to 100 m (indoor), Lower transmit power, Full channel width (20+ MHz)
Latency	<1 ms	30–50 ms	10–100 ms
Security	High with dedicated enterprise measures	High but shared with public users	Moderate with WPA3 encryption
Capacity	Up to 10 Gbps	1–3 Gbps	100–300 Mbps
Scalability	Millions of devices	Thousands of devices per cell	Limited to dozens of devices
Control	High (enterprise-controlled)	Low (operator-controlled)	High (Enterprise-controlled)
Reliability	99.999% (SLAs)	99.99% (network load dependent)	99%
Customization	High	Low	Low
Use case suitability	Industry-specific, mission-critical applications	General public use	Home, small businesses
Cost	Moderate initial investment, lower long-term cost	High operational cost	Low equipment cost
Traffic handling	Scheduled, Weighted Upload/Download	Managed, Prioritized Traffic	Distributed contention
Quality of service	Deterministic, Mandatory RF Feedback Loop	High QoS with SLA	Statistical prioritization
Density handling	Dual Factor OFDMA, Non-Blocking interference	Optimized for urban environments	Single factor OFDMA, Blocking interference
Mobility	Precisely timed handovers	Seamless mobility, Managed handoffs	Client off-channel scanning, Client-Controlled roaming

and Wi-Fi, which requires client off-channel scanning, making it less efficient for mobile applications [38].

Let us compare a theoretical deployment of private 5G CBRS versus Wi-Fi 6E in a large industrial environment, such as a manufacturing plant with 250,000 square feet indoors and 1,000,000 square feet outdoors. For indoor coverage, a private 5G network would require only 25 APs at $7000 each, totaling $175,000, whereas Wi-Fi 6E would need 100 APs at $2100 each, costing $210,000. For outdoor coverage, private 5G needs just 5 APs ($35,000 total), while Wi-Fi demands 40 APs at a total cost of $164,000. Hardware costs also favor 5G CBRS, totaling $375,000 for APs, CBRS core, and network management, compared to Wi-Fi's range of $43,000 to $434,000, largely due to Wi-Fi's higher AP and controller needs.

Installation costs reinforce 5G CBRS's advantage: while both networks require $1000 per AP for indoor installation, outdoor setup costs are $60,000 for 5G CBRS versus $236,000 for Wi-Fi. In terms of reliability, 5G CBRS offers a 99.9% SLA, resulting in only 8.76 h of downtime per year, compared to Wi-Fi's 99% SLA with 87.6 h of downtime. Private 5G also supports critical applications through Mobile Edge Computing (MEC) at $20,000–$30,000 per server, which Wi-Fi lacks.

Maintenance costs for both networks are estimated at 12% of initial hardware and software annually. For client devices, private 5G requires Band 48 CPEs with SIM cards ($43,000 annually), while Wi-Fi 6E CPE costs are slightly higher at $52,000 annually. This comparison highlights how private 5G CBRS, with fewer APs, lower installation costs, and superior reliability, is better suited for large-scale industrial applications than Wi-Fi 6E, providing cost-efficiency and robust performance in mission-critical environments.

To further illustrate the practical differences between private 5G using CBRS and Wi-Fi 6E in industrial settings, Table 7 summarizes key aspects such as spectrum, cost, hardware, and scalability. This comparison reinforces why CBRS-based private 5G is more efficient and cost-effective for large-scale, mission-critical deployments.

In addition to the detailed cost comparison already presented in Table 6, we further clarify that private 5G networks benefit from the use of semi-licensed spectrum, which is available at no direct cost to the operator. This contrasts with Enterprise Wi-Fi, which relies on unlicensed spectrum that may be subject to interference and does not inherently provide the same cost advantages. By leveraging a dedicated spectrum arrangement for private 5G, the overall expense associated with acquiring spectrum rights is minimized, thereby reducing the total cost of ownership. Moreover, private 5G networks are designed to offer extensive coverage; a single base station can often cover a much larger area compared to a Wi-Fi access point. This feature significantly reduces the number of hardware units needed per square mile, bringing down installation, cabling, and ongoing maintenance costs.

Furthermore, when evaluating scalability for large industrial or campus environments, the difference in deployment density between private 5G and Enterprise Wi-Fi becomes even more pronounced. While Wi-Fi typically requires many access points to cover a large area – especially when reliable, high-capacity service is needed – the superior propagation characteristics and advanced beamforming capabilities of 5G allow for broader coverage with fewer units. This scalability advantage means that, despite a higher initial investment for the 5G core and related infrastructure, the long-term operational costs are lower due to reduced hardware requirements and simplified network management. Additionally, as more countries allocate spectrum for private 5G, the economic benefits of this approach are expected to grow further.

5.1. The benefits of spectrum sharing and CBRS

The CBRS framework exemplifies the benefits of spectrum sharing by maximizing the utility of the mid-band spectrum, a scarce and valuable resource. By allowing commercial users to access frequencies otherwise reserved for government use, spectrum sharing reduces the cost and regulatory burden of acquiring exclusive spectrum licenses. For private networks, especially those deployed in industrial, logistics,

Table 7
Comparison of CBRS and Wi-Fi 6E in industrial deployment context.

Aspect	CBRS (Private 5G)	Wi-Fi 6E
Spectrum type	Semi-licensed (3.5 GHz) with SAS coordination	Unlicensed (2.4/5/6 GHz)
Spectrum cost	Free (no license fee)	Free (no license fee)
Coverage per AP	High (large indoor/outdoor range)	Low (small indoor range, needs dense deployment)
Number of APs (Indoor)	Approx. 25 for 250,000 sq. ft.	Approx. 100 for 250,000 sq. ft.
Number of APs (Outdoor)	Approx. 5 for 1,000,000 sq. ft.	Approx. 40 for 1,000,000 sq. ft.
AP cost	$7000 per unit	$2100 per unit
Core network	Required (CBRS Core)	Not required (decentralized)
Installation cost	Lower (fewer APs, centralized control)	Higher (more APs, more wiring)
Maintenance cost	12% of hardware/software	12% of hardware/software
Client hardware	Band 48 CPE with SIM ($43k/year)	Standard Wi-Fi 6E CPE ($52k/year)
SLA reliability	99.9% (approx. 8.76 h downtime/year)	99% (approx. 87.6 h downtime/year)
Scalability	High (millions of devices)	Moderate (limited by interference and density)
Security	High (SIM-based, enterprise controlled)	Moderate (WPA3 encryption)

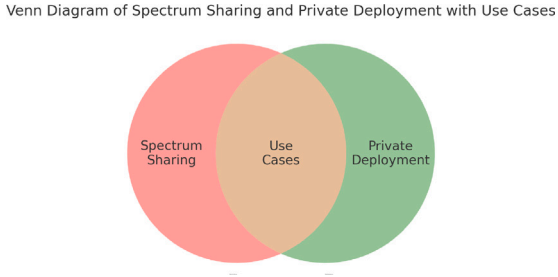

Fig. 5. Venn diagram of spectrum sharing and private deployment with use cases: This diagram shows the overlap between spectrum sharing and private deployment, with use cases positioned at the intersection, indicating their reliance on both elements for feasibility.

and manufacturing environments, CBRS offers a solution to the limitations of Wi-Fi and public cellular networks. The shared 3.5 GHz band enables enterprises to establish robust private networks with dedicated, interference-free bandwidth, suitable for data-intensive applications and real-time connectivity.

Since its official launch by the FCC in 2019, CBRS has opened new possibilities for deploying private LTE and 5G networks across a wide range of industries. The combination of spectrum sharing and CBRS has created a model that benefits not only primary and secondary users but also accelerates innovation in sectors requiring reliable, high-performance connectivity. This collaborative approach to spectrum use has the potential to shape future regulatory practices, as countries worldwide explore similar shared spectrum frameworks to address the growing demand for wireless communication.

6. Applications deployed in private networks with spectrum sharing

In an increasingly connected world, private networks and spectrum sharing enhance performance and accessibility for various applications. Private deployments provide dedicated resources for superior security, reliability, and speed, while spectrum sharing optimizes frequency use for multiple users. This section explores the benefits of these technologies in immersive AR/VR experiences, smart city infrastructure, and public safety networks, highlighting their role in driving innovation and operational excellence across sectors.

As shown in Fig. 5, use cases depend on the integration of both spectrum sharing and private deployment. Spectrum sharing optimizes frequency band usage, crucial for high-demand wireless environments. Private deployment provides dedicated resources, enhanced security, and customization. Without spectrum sharing, there would not be enough spectrum for applications like AR, VR, industrial automation, smart grids, autonomous vehicles, remote healthcare, IoT devices, and real-time data analytics. Without private deployment, meeting the specific needs of various industries would be impractical, rendering many use cases unfeasible.

6.1. Applications for private deployments with spectrum sharing

6.1.1. Augmented Reality (AR)

Augmented reality (AR) is transforming industries by enabling real-time, interactive experiences that depend on low-latency, high-bandwidth connectivity. Private networks support seamless AR performance by providing dedicated bandwidth, essential for high-speed data transmission without interruptions. In manufacturing, for instance, AR overlays assist workers with step-by-step instructions during complex tasks, boosting productivity and accuracy. The automotive sector leverages AR for heads-up displays in vehicles, while medical training relies on AR to simulate intricate procedures with real-time feedback. Retail also benefits, as private networks support AR-based virtual try-ons, enhancing customer experience. Spectrum sharing ensures multiple AR applications can operate efficiently, underscoring private networks' role in delivering reliable, high-performance AR services across diverse environments.

6.1.2. Virtual Reality (VR)

Virtual reality (VR) applications demand substantial bandwidth and low latency to deliver immersive, responsive experiences, which private networks are well-equipped to support. Private 5G networks ensure stable, high-speed connectivity, critical for VR training simulations, gaming, virtual tourism, and therapeutic applications in healthcare. In aviation, VR systems provide pilots with realistic training simulations, relying on private networks to maintain low-latency, high-bandwidth connections. Spectrum sharing optimizes bandwidth, enabling cost-effective access to high-performance VR resources, making private networks invaluable for industries leveraging VR for training, entertainment, and remote experiences.

6.1.3. Industrial automation

Industrial automation relies on real-time, reliable data exchange between machines and control systems to optimize production processes. Private networks meet these stringent requirements, delivering

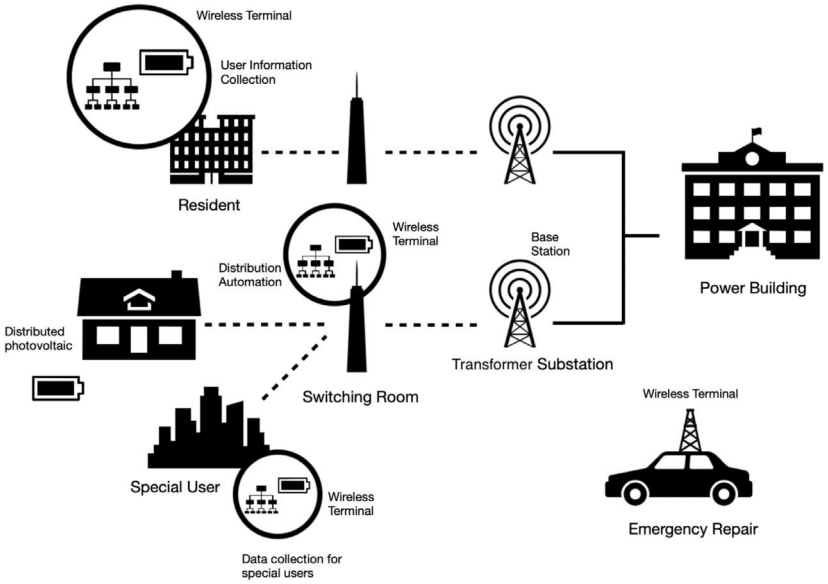

Fig. 6. An illustration of a power wireless private network in an energy IoT setup shows components like user information collection, distribution automation, and data collection for special users integrated using wireless terminals and base stations. This setup ensures reliable and secure communication, crucial for efficient operations in the energy sector.

low latency and high bandwidth crucial for robotics, assembly lines, and automated quality control. For example, food and beverage production facilities use automated systems for precise packaging, where private networks support seamless communication for efficiency. Spectrum sharing enables uninterrupted operation in high-density environments, ensuring private networks enhance productivity, safety, and automation quality across industries.

6.1.4. IoT devices

The growth of IoT devices in industry and infrastructure requires robust, scalable networks capable of managing high data volumes and device densities. Private networks address these needs by providing reliable, secure connectivity, crucial for applications like predictive maintenance, smart farming, and city infrastructure. For instance, smart energy grids employ private networks to collect and manage real-time data for efficient distribution (see Fig. 6). Spectrum sharing enhances network flexibility, allowing private networks to support extensive IoT ecosystems and ensure scalability and operational efficiency.

6.1.5. Real-time data analytics

Real-time data analytics, essential for applications requiring immediate decision-making, depends on high-speed data transmission and processing capabilities. Private networks provide the necessary bandwidth and low latency to perform analytics without delay, ensuring fast insights in sectors like finance, retail, and logistics [120]. In healthcare, for example, real-time patient monitoring relies on quick data processing for responsive treatment decisions. Spectrum sharing enhances network efficiency by allowing simultaneous data set analysis, making private networks integral to timely, accurate analytics across industries (see Fig. 7).

6.1.6. Autonomous vehicles

Autonomous vehicles (AVs) require reliable, low-latency communication to function safely and effectively. Private networks support the high-speed, stable connections necessary for vehicle-to-everything (V2X) interactions, while spectrum sharing enhances network availability in high-demand areas [121,122]. Self-driving cars, delivery drones, and agricultural vehicles rely on private 5G for real-time data and navigation. For instance, autonomous drones used in emergency response scenarios benefit from private networks' stable communication for remote control and data processing (see Fig. 8) [123]. This connectivity ensures reliable AV operations, bolstering safety and efficiency.

6.1.7. Transportation management

Transportation management systems benefit from private networks, which provide real-time data exchange critical for optimizing schedules, reducing congestion, and enhancing safety [124–126]. Private 5G networks support applications such as real-time public transport tracking, traffic signal optimization, and fleet management, ensuring efficient communication across systems. Autonomous buses, for example, rely on stable connections for route planning and safety. Spectrum sharing further enhances these operations, allowing multiple applications to coexist efficiently, improving overall transportation logistics and reducing delays (see Fig. 9).

6.2. Customer need use cases for private deployments with spectrum sharing

6.2.1. Oil and gas

The oil and gas sector operates in remote, challenging environments where reliable connectivity is essential. Private networks provide the necessary resilience, supporting operations such as remote monitoring of drilling platforms, pipeline leak detection, and environmental monitoring [127–129]. Spectrum sharing maximizes frequency use, ensuring continuous, efficient communication. Private networks with spectrum sharing enhance safety, efficiency, and responsiveness across oil and gas operations (see Fig. 10).

6.2.2. Super centers and retail

Retail environments require robust connectivity for inventory management and customer engagement. Private networks support real-time tracking, smart fitting rooms, and dynamic pricing, with spectrum sharing ensuring efficient network use in high-density areas [130–132]. This integration enhances operational efficiency and customer satisfaction in large retail environments, as illustrated by Walmart's deployment (see Fig. 11).

6.2.3. Airports

Airports need reliable, congestion-free communication for passenger information, security, and ground operations. Private networks ensure seamless updates, baggage handling, and surveillance, with spectrum sharing enhancing service quality in high-traffic areas [134,135]. Frankfurt Airport, for example, uses Europe's largest private 5G network for autonomous operations (see Fig. 12).

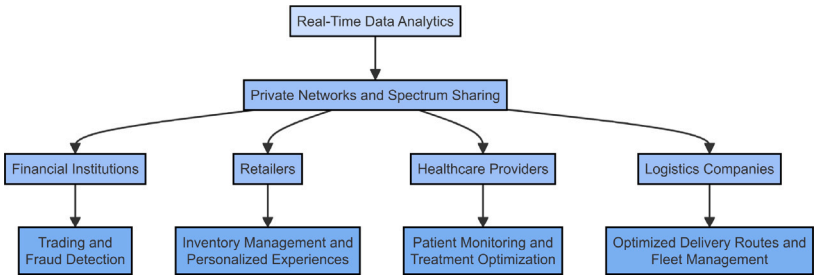

Fig. 7. Illustration of real-time data analytics applications across different sectors. Private networks and spectrum sharing can be utilized in settings like these to enhance data processing and transmission.

Fig. 8. Autonomous drones can be used as first responders powered by private 5G networks [123], providing real-time data analysis and efficient operations.

6.2.4. Ship ports

Ship ports rely on robust and resilient connectivity to support complex logistics operations, efficient container tracking, and secure communication channels, which are critical for handling the vast flow of goods passing through these facilities. Private networks provide the high-speed, low-latency connections needed for real-time data transmission, allowing for continuous monitoring and operation of automated machinery such as cranes, AGVs (Automated Guided Vehicles), and other equipment that streamline cargo movement. Additionally, private networks ensure that all equipment and personnel within the port are connected for seamless coordination and safety. Spectrum sharing further enhances connectivity by optimizing the use of available frequency bands, reducing interference in high-density environments where numerous devices are in constant communication. This integration of private networks with spectrum sharing significantly optimizes port operations, boosting efficiency and reliability.

6.2.5. Warehouses

Warehouses leverage private networks to facilitate a high degree of automation and real-time inventory management, both essential for the seamless operation of AGVs (Automated Guided Vehicles), robotics, and other smart logistics solutions. Private networks ensure stable, low-latency connections that enable continuous, real-time data exchange, supporting precise AGV navigation and efficient robotic workflows across warehouse facilities. Additionally, private networks allow seamless communication among various devices, such as scanners, conveyors, and inventory systems, ensuring that every part of the process is synchronized for maximum productivity. Spectrum sharing further boosts connectivity by optimizing available frequencies, making it possible to support large numbers of devices in high-density environments, thus enhancing operational accuracy, scalability, and flexibility. This integration allows warehouses to operate at peak efficiency and manage fluctuating demands with ease, as shown in Fig. 13 [136,137].

6.2.6. Factories

Factories depend on highly reliable communication networks to enable real-time production monitoring and support advanced automation processes essential for modern manufacturing. Private networks provide the low-latency, high-speed connectivity required for predictive maintenance, allowing equipment to be monitored continuously and potential issues to be addressed before they cause downtime. This connectivity also facilitates synchronized operations across various stages of production, ensuring that processes are coordinated and efficient. Spectrum sharing further enhances these private networks by maximizing available bandwidth and reducing interference, which is particularly valuable in dense factory environments with numerous connected devices. This combination of private networking and spectrum sharing elevates manufacturing efficiency, quality, and responsiveness.

6.2.7. Healthcare in hospitals

Hospitals require secure, low-latency networks to support critical patient care applications, and private networks fulfill this need by providing the reliable connectivity essential for healthcare environments. These networks enable seamless access to electronic health records (EHR), real-time telemedicine services, and continuous monitoring in intensive care units (ICUs), ensuring that healthcare providers can deliver responsive and efficient care. Spectrum sharing further enhances this connectivity by optimizing bandwidth usage, which is particularly beneficial in both densely populated urban hospitals and remote rural facilities. This shared spectrum approach ensures consistent, high-quality connectivity across all locations, allowing for uninterrupted patient data access and communication. The integration of private networks and spectrum sharing is vital for the advanced technological capabilities of smart hospitals, as illustrated in Fig. 14 [138].

6.2.8. Universities

Universities benefit significantly from private networks, which support a wide range of educational technologies and ensure secure data sharing in research labs and collaborative projects. These networks provide the reliable, high-speed connectivity needed for online learning platforms, enabling students and faculty to access digital resources, participate in virtual classrooms, and engage in real-time discussions. Additionally, private networks bolster campus security through IoT-enabled surveillance and automated access control, ensuring a safe and efficient campus environment. Spectrum sharing further enhances network performance by optimizing connectivity across large and densely populated campuses, supporting the simultaneous demands of online learning, administrative operations, and research activities without interference. This integration enables universities to foster an advanced, connected learning environment, as depicted in Fig. 15.

6.2.9. Distribution centers

Distribution centers depend on private networks to support real-time package tracking, automated sorting systems, and efficient inventory management, all of which are essential for fast-paced logistics operations. These private networks provide the reliable connectivity required to monitor inventory levels continuously, track packages throughout the facility, and coordinate sorting processes in real time. This level of connectivity ensures that items are processed accurately and efficiently, reducing errors and minimizing delays. Spectrum sharing further enhances the network by optimizing frequency usage, allowing multiple devices and systems to operate simultaneously without

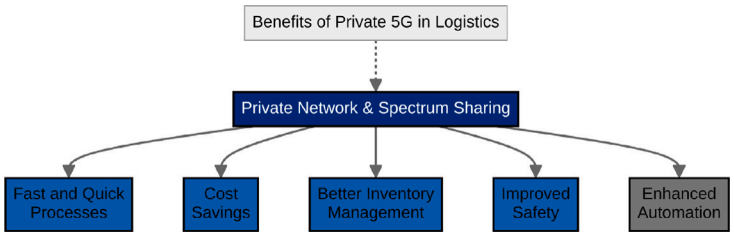

Fig. 9. Benefits of private 5G in logistics: This figure shows how private networks and spectrum sharing improve logistics through faster processes, cost savings, better inventory management, improved safety, and enhanced automation.

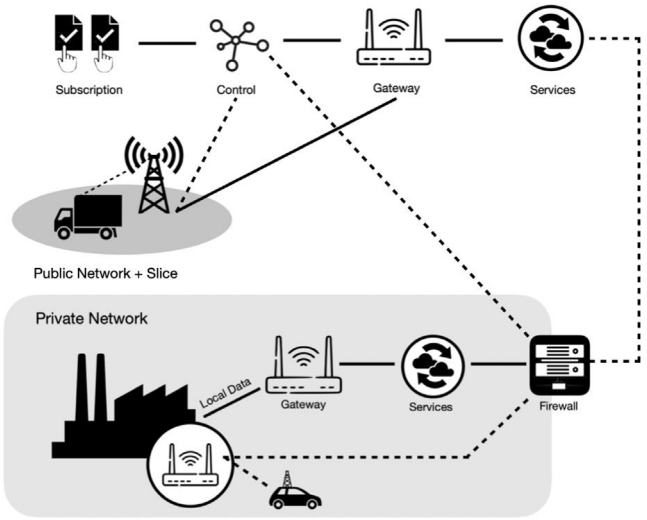

Fig. 10. Integration of private networks in oil and gas for real-time monitoring and control between remote sites and control centers.

Fig. 11. Real-time inventory tracking at Walmart using private networks [133].

Fig. 12. Private 5G at Frankfurt Airport supports autonomous driving and efficient data communication [135].

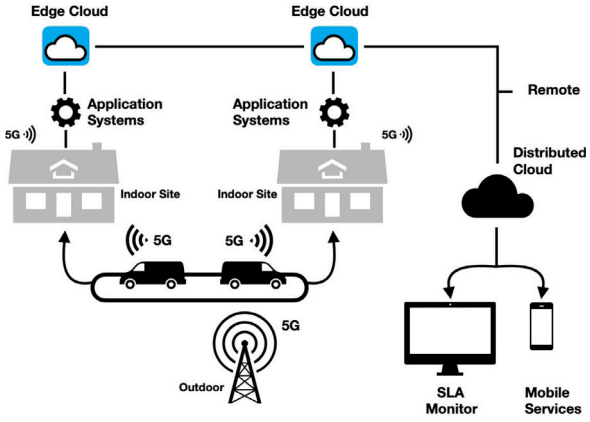

Fig. 13. Private networks enable real-time tracking, automation, and coordination in warehouses.

interference. This combination improves overall accuracy, productivity, and logistical efficiency, enabling distribution centers to meet high demand and streamline operations, as shown in Fig. 16 [140,141].

6.2.10. Remote healthcare services

Remote healthcare services, including telemedicine and patient monitoring, rely on private networks to ensure secure, low-latency connectivity essential for high-quality patient care. These networks support real-time consultations, allowing healthcare providers to offer timely advice and diagnostics regardless of the patient's location, and they facilitate continuous monitoring for patients with chronic conditions, enabling immediate intervention if needed. Spectrum sharing enhances the effectiveness of private networks by optimizing frequency usage, which is particularly beneficial in remote areas where connectivity options may be limited. This integration ensures reliable communication and data exchange, making remote healthcare a viable and efficient option for many patients, as shown in Fig. 17.

6.2.11. Smart cities

Smart cities depend on seamless private networks to support a range of integrated applications, including traffic management, public safety initiatives, and environmental monitoring systems, all of which contribute to improved urban living and resource management. These private networks provide the high-speed, reliable connectivity needed for real-time data sharing between various city services, allowing for dynamic responses to changing conditions, such as traffic flow adjustments or emergency service coordination. Spectrum sharing further enhances network efficiency by optimizing bandwidth use in densely populated urban areas, ensuring that numerous connected devices and

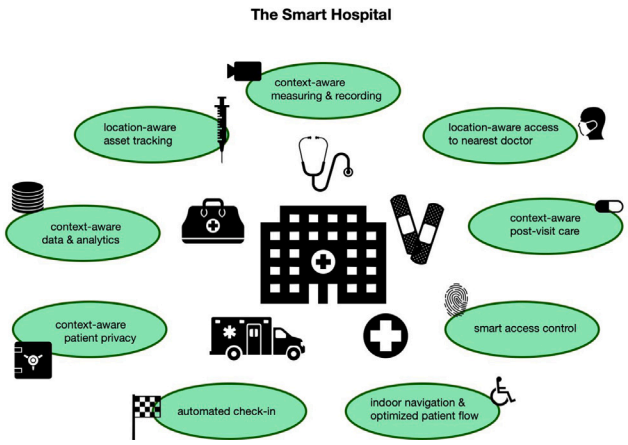

Fig. 14. Smart hospital supported by private networks for enhanced care and operational efficiency.

Fig. 15. Universities use private networks for secure, high-speed research and education support [139].

Fig. 16. Private networks support logistics and inventory management in distribution centers [142].

applications can operate without interference. This integration enables smart cities to function more smoothly, supporting sustainable urban development and enhancing the quality of life for residents, as illustrated in Fig. 18 [143,144].

6.2.12. Agriculture

Agricultural operations gain substantial advantages from private networks, which enable precision farming practices and real-time monitoring essential for effective management of environmental sensors, automated machinery, and livestock tracking systems. These networks provide reliable, high-speed connectivity, allowing farmers to make data-driven decisions on irrigation, fertilization, and pest control based

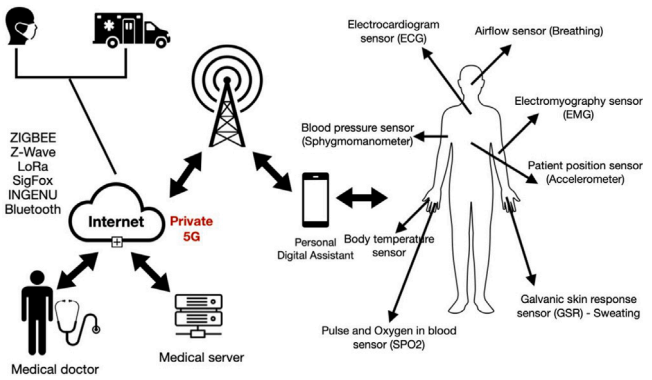

Fig. 17. Remote healthcare relies on private networks for secure, real-time patient data transmission.

on real-time conditions, thereby optimizing crop yield and resource use. Automated equipment, such as drones and autonomous tractors, relies on private networks to operate seamlessly, ensuring precise and efficient fieldwork. Spectrum sharing enhances connectivity in rural areas by optimizing frequency use, which is crucial for supporting extensive agricultural operations across large fields and remote locations. This integration improves resource management and overall productivity.

6.2.13. Enterprise

Modern enterprises leverage private networks to enable IoT-driven workspaces, advanced security systems, and automated building management solutions, all of which contribute to streamlined operations and a more responsive work environment. Private networks provide the secure and reliable connectivity needed to support a wide range of applications, from smart lighting and HVAC systems that adapt to occupancy levels, to access control and surveillance systems that ensure workplace security. Spectrum sharing further optimizes connectivity, enabling seamless communication among numerous devices within high-density office settings, thereby enhancing operational efficiency, energy management, and security. This integration fosters a smarter, more sustainable office environment, as illustrated in Fig. 19.

7. Challenges in private 5G deployment and mitigation strategies

Before delving into the challenges associated with private 5G deployments, it is important to clarify the role of Open Radio Access Network (ORAN) in this context. ORAN represents a paradigm shift in network architecture by promoting interoperability through multi-vendor hardware and software components. While ORAN offers increased flexibility and the potential for cost reduction through open standards, it also introduces substantial complexity. Integrating diverse radio units, baseband units (BBUs), and connecting them to a centralized 5G core (CU/DU) demands new deployments and a higher number of hardware components compared to existing infrastructures such as Enterprise Wi-Fi. These challenges – including increased costs, more complex system management, and the need for additional new hardware – explain why ORAN has become a significant challenge in the deployment of private networks.

Deploying private 5G networks offers significant benefits, but it also presents various technical, operational, and financial challenges. Key obstacles in private 5G deployment include the high costs of hardware and software, the complexity of integrating ORAN components from multiple vendors, interoperability issues, system stability, and the need for robust security mechanisms. This section explores these challenges in detail and outlines strategies to mitigate them.

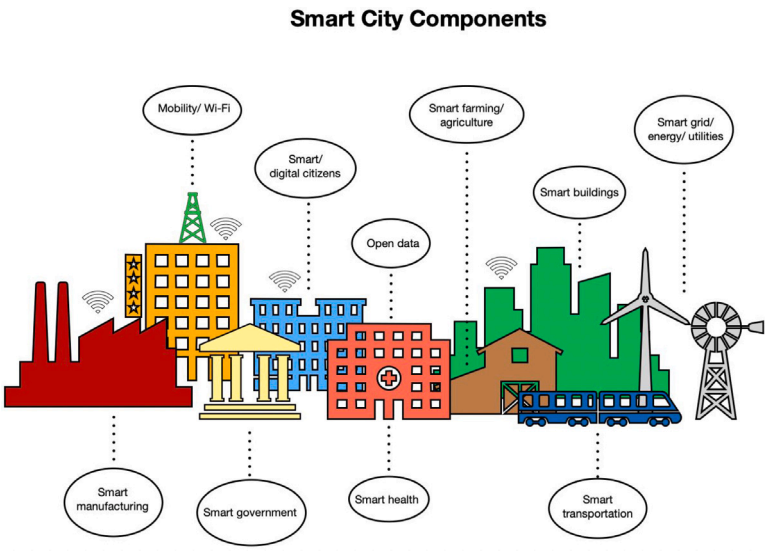

Fig. 18. Smart cities use private networks for integrated applications enhancing efficiency and livability.

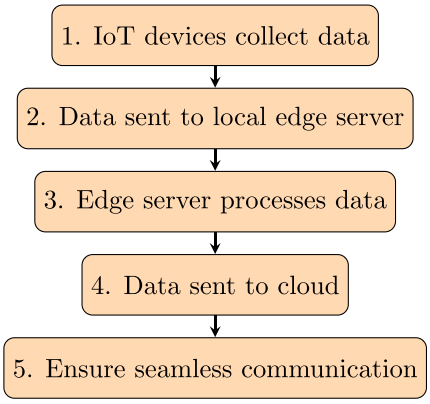

Fig. 19. Integration of private networks in a smart office building.

7.1. Cost and complexity of hardware and software

Challenge: Deploying private 5G networks requires substantial investment in specialized hardware and software, including RAN equipment, core network components, and edge computing infrastructure. The costs associated with these components, coupled with the complexity of installation and maintenance, create barriers for many organizations. Furthermore, specialized expertise is often required to configure and optimize these systems, adding to operational expenses.

Mitigation Strategy: To address these cost and complexity issues, organizations can explore managed services or Network-as-a-Service (NaaS) models, which reduce upfront costs by offering infrastructure on a subscription basis. Additionally, selecting vendors that provide modular, scalable solutions can allow companies to incrementally build their networks in stages, optimizing their budgets. Finally, leveraging virtualized and software-defined networking (SDN) technologies can help streamline network management and reduce reliance on costly proprietary hardware.

7.2. Interoperability and integration challenges with multi-vendor solutions

Challenge: Private network deployments face significant interoperability challenges when integrating components from multiple vendors, regardless of whether they follow ORAN (Open Radio Access Network) principles or traditional architectures. The fundamental issue lies in multi-vendor integration rather than being specific to any particular technology approach. When end-to-end solutions combine components from different vendors – such as access points from one vendor with 5G core networks from another – substantial compatibility issues arise. These challenges include complex troubleshooting processes, coordinated software releases for end-to-end verification, synchronized bug fixes across vendors, and difficulties in implementing new features that require seamless interaction between different vendor systems.

Single-vendor solutions typically provide better compatibility and streamlined operations, as all components are designed and tested to work together. In contrast, multi-vendor deployments can be characterized as a "frankenstein method", where determining the root cause of issues becomes challenging for customers, as problems could originate from any vendor's component or from the interaction between different vendors' systems. Additionally, rigorous testing becomes significantly more time-consuming and complex when multiple vendors are involved, as each integration point must be thoroughly validated.

Mitigation Strategy: Organizations have several strategic options to address multi-vendor integration challenges. The most straightforward approach is to select integrated solutions where all major components (radio access, edge computing, and core network) are provided by a single vendor, thereby ensuring optimal compatibility and simplified maintenance. For organizations that prefer multi-vendor flexibility, employing experienced system integrators who specialize in complex network deployments can help manage the integration challenges and minimize compatibility issues. Additionally, implementing comprehensive testing frameworks and establishing clear vendor responsibility matrices can help streamline troubleshooting and maintenance processes.

7.3. Stability of softwarized RAN on general purpose compute

Challenge: Private 5G networks increasingly rely on softwarized RAN (Radio Access Network) components, which often operate on general-purpose computing infrastructure. While this approach offers flexibility and cost benefits, it can also introduce stability concerns. General-purpose compute platforms may not be optimized for high-performance, latency-sensitive RAN operations, leading to potential performance degradation and reliability issues.

Mitigation Strategy: To enhance the stability of softwarized RAN, organizations can leverage specialized hardware acceleration techniques, such as using FPGAs (Field-Programmable Gate Arrays) or

GPUs (Graphics Processing Units), to offload critical processing tasks. Additionally, implementing strict Service Level Agreements (SLAs) with vendors can ensure that performance benchmarks are met. Collaborating with vendors who specialize in optimizing software for RAN on general-purpose compute can also help improve system stability and performance.

7.4. Control domain complexity

Challenge: The control architecture in private 5G networks involves multiple, often disparate, control domains. These include RAN control, 5G core control, user equipment (UE) management, and interconnecting network control, among others. Integrating and managing these control domains within a unified framework is challenging and can lead to configuration and operational inefficiencies. Mismanagement of these control domains may result in network performance issues, including latency and inconsistent quality of service (QoS).

Mitigation Strategy: To address the complexity of multiple control domains, organizations can deploy centralized management systems that integrate with and provide visibility across all control domains. Software-defined networking (SDN) and network function virtualization (NFV) technologies can also help unify control across different network components. Additionally, adopting standardized protocols and interfaces, such as those promoted by the ORAN Alliance, can improve interoperability and simplify control domain management.

7.5. Security concerns in private 5G networks

Challenge: Security is a critical concern in private 5G networks, especially given the high value and sensitivity of data traversing these systems. Private 5G networks face risks such as unauthorized access, data breaches, and cyber-attacks targeting network infrastructure. The presence of multi-vendor environments in ORAN deployments also complicates security management, as each vendor may have different security practices and protocols. Furthermore, softwarized and virtualized network components are more vulnerable to software-based attacks.

Mitigation Strategy: To enhance security, organizations should implement robust security frameworks that include multi-layer encryption, network segmentation, and stringent access controls. Security information and event management (SIEM) systems can be deployed to monitor network activity in real-time, detecting and mitigating threats as they arise. Adopting a Zero Trust Architecture (ZTA) can also improve security by enforcing strict identity verification at every stage of the network. Additionally, selecting vendors who adhere to industry security standards, such as the ORAN Alliance's security specifications, can help address vulnerabilities within multi-vendor deployments.

7.6. Need for system integrators

Challenge: The deployment of private 5G networks requires expertise across a wide range of technical domains, including RAN, edge computing, network orchestration, and cybersecurity. As such, organizations often need the assistance of specialized system integrators to coordinate between vendors, configure systems, and ensure interoperability. This dependency on system integrators adds both cost and complexity to the deployment process.

Mitigation Strategy: To reduce reliance on system integrators, companies can invest in training their IT and networking teams to develop expertise in 5G technologies, allowing them to manage deployments in-house. Additionally, choosing vendors who provide end-to-end solutions can simplify integration by reducing the need for third-party coordination. For organizations opting for multi-vendor setups, partnering with system integrators who offer flexible, as-needed support can help control costs while ensuring access to expert guidance when necessary.

8. Future of private networks

The evolution of private networks is set to revolutionize the way enterprises operate, offering unparalleled performance, reliability, and security. The future of private networks is driven by several key advancements, including enhanced spectrum utilization, next-generation spectrum technologies, and the advent of private 6G networks.

8.1. Enhanced spectrum utilization

Enhanced spectrum utilization is a cornerstone of the future of private networks. With the increasing demand for wireless connectivity, the efficient use of available spectrum has become critical. The National Spectrum Consortium (NSC) proposes to extend its successful PATHSS initiative by creating a permanent Spectrum Roundtable, utilizing its diverse membership and administrative infrastructure to facilitate collaborative spectrum management and innovation, and offering a pathway for testing and prototyping spectrum-based technologies to support NTIA's ambitious National Spectrum Strategy [145].

The demand for increased spectrum is driven by the proliferation of connected devices and the growing need for high-speed, reliable wireless communication in various industries. The 5G CONNI Europe–Taiwan project aims to enhance global manufacturing competitiveness by developing and validating innovative Private 5G solutions, architectures, and technologies tailored for Industry 4.0, offering an integrated end-to-end testing network for industrial applications across interconnected sites in Taiwan and Europe [146].

Carrier aggregation for private 5G networks is a key technology that allows for the combination of multiple spectrum bands to increase bandwidth and improve network performance. This technology enables private networks to meet the high demands of modern industrial applications, providing the necessary capacity and reliability. The capabilities of existing radios are continuously being enhanced to support these advanced features, ensuring that private networks can leverage the available spectrum to its fullest potential.

However, there is a need for future spectrum allocations to keep pace with the growing demands of private networks. The Department of Defense (DoD) is advancing its 5G deployments and exploring dynamic spectrum sharing to support military systems and expand wireless capabilities, focusing on collaboration with commercial partners and mitigating interference with radar systems [147,148]. This collaborative approach is essential to ensuring that both military and commercial needs are met, paving the way for efficient spectrum utilization.

CTIA stresses the importance of a spectrum strategy that includes allocating additional full-power commercial wireless licensed spectrum to bolster national security and economic growth. They highlight the U.S. wireless industry's $825 billion GDP contribution in 2020 and the need to keep pace with international allocations where the U.S. currently lags behind by an average of 378 MHz. They advocate for legislative and regulatory modifications to the Spectrum Relocation Fund, proposing expedited disbursement and increased flexibility to facilitate spectrum reallocation and technology upgrades for the DoD [149].

8.2. Next-Generation Spectrum (NGS)

Next-Generation Spectrum (NGS) is poised to be a game-changer for private networks, offering new possibilities for enhanced performance and reliability. NGS encompasses advanced spectrum technologies and innovative allocation models that are critical for the development of future private networks.

The definition and importance of NGS lie in its ability to support the next wave of technological advancements. Potential bands and frequencies for NGS include higher frequency ranges that can provide greater bandwidth and lower latency, essential for applications such as autonomous vehicles, advanced manufacturing, and immersive virtual reality experiences.

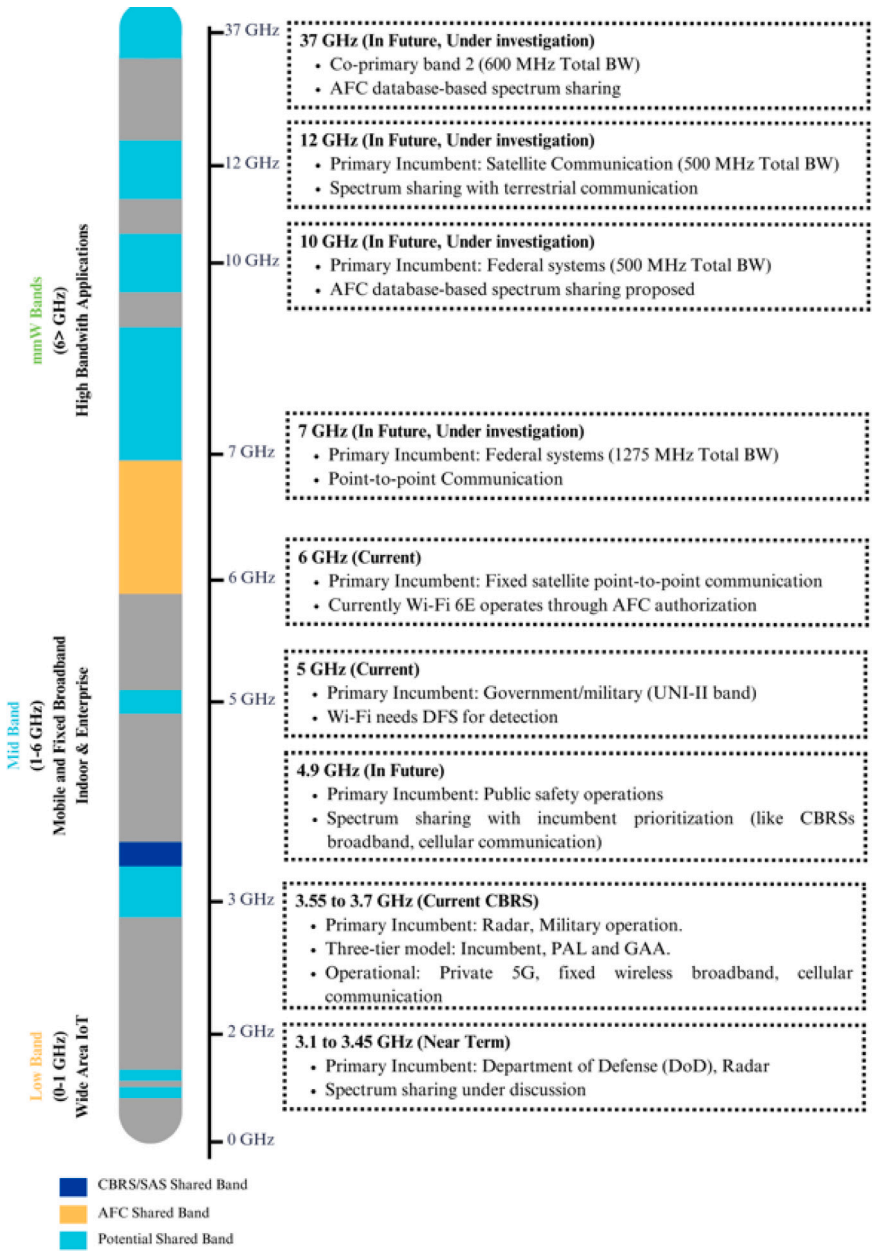

Fig. 20. Opportunities in the Unlicensed Spectrum across different frequency bands.

Fig. 20 explains the current and future state of spectrum sharing across various frequency bands, highlighting different incumbents and applications. The 37 GHz band, currently under investigation, is proposed as a co-primary band with 600 MHz total bandwidth, utilizing AFC database-based spectrum sharing. The 12 GHz and 10 GHz bands, also under investigation, have primary incumbents in satellite communication and federal systems respectively, with proposals for spectrum sharing. The 7 GHz band is under investigation for federal systems and point-to-point communication, while the 6 GHz band is currently utilized for fixed satellite point-to-point communication, with Wi-Fi 6E operating through AFC authorization. In the 5 GHz band, government and military use the UNII-II band with Wi-Fi requiring DFS for detection. The 4.9 GHz band is set for future use by public safety operations with spectrum sharing similar to CBRSs broadband and cellular communication. The 3.55 to 3.7 GHz CBRS band operates under a three-tier model for radar and military operations, supporting private 5G and fixed wireless broadband. The 3.1 to 3.45 GHz band is under near-term consideration for Department of Defense and radar use with potential spectrum sharing. The figure also categorizes applications by frequency: high-bandwidth applications above 6 GHz (mmW/High Band), wide-area IoT below 1 GHz (Low Band), and mobile and fixed broadband, including Wi-Fi bands between 1 to 6 GHz (Mid Band). A legend distinguishes CRBS/ASA shared bands in dark blue, AFC shared bands in orange, and potential shared bands in light blue.

Technological advancements in NGS are driving the development of more efficient and dynamic spectrum sharing models. The DoD is working on a "moonshot" project to develop a dynamic spectrum sharing (DSS) framework for the 3.1–3.45 GHz band over the next 12–18 months, aiming to balance national security and commercial wireless needs. This initiative follows the successful auction of the 3.45–3.55 GHz spectrum, which raised $21 billion, and involves collaboration with the NTIA, industry, and academia to create an effective DSS system [150].

Regulatory considerations are crucial in the implementation of NGS. The DoD released a redacted report in April 2024 indicating that sharing the 3.1–3.45 GHz band for 5G is currently infeasible without

specific regulatory, technological, and resource conditions. The report emphasizes the need for a comprehensive coordination framework and safeguards to ensure both military and commercial operations can coexist effectively [151].

Innovative spectrum allocation models are being explored to maximize the use of available spectrum. The National Spectrum Consortium (NSC) has launched the Partnering to Advance Trusted and Holistic Spectrum Solutions (PATHSS) Task Group to collaborate with the DoD on exploring spectrum sharing solutions in the 3.1–3.45 GHz band for commercial 5G, facilitating sensitive information exchange and fostering trust among stakeholders. This initiative aims to develop realistic spectrum sharing implementations and provide insights to support both 5G development and military needs [152].

The impact of NGS on network performance and reliability cannot be overstated. The Department of Defense's 2023 report on the feasibility of sharing the 3.1–3.45 GHz spectrum band highlighted significant operational challenges, stating that sharing is currently infeasible without regulatory, technological, and resourcing changes. The ongoing debate in Congress focuses on balancing DoD needs with expanding commercial wireless services, with potential solutions including maintaining Section 90008 of the IIJA for further study or reallocating the spectrum for nonfederal use, which could generate substantial auction revenues but require costly modifications to DoD systems [153].

The future of private networks hinges on advancements in spectrum utilization and the development of next-generation spectrum technologies. These innovations will enable private networks to deliver unparalleled performance, reliability, and security, supporting a wide range of industrial and commercial applications. The collaborative efforts between industry, government, and academia are essential to achieving these goals and ensuring that the benefits of private networks are fully realized.

8.3. Prospective private 6G networks

As we look toward the future, private 6G networks are poised to revolutionize connectivity and provide unprecedented capabilities for various industries. The vision for private 6G encompasses not only enhanced performance and reliability but also the integration of advanced technologies to meet the evolving demands of modern enterprises.

8.3.1. Vision for private 6G

The vision for private 6G networks is to create a seamless, intelligent, and highly adaptive network infrastructure that can support a diverse range of applications and use cases. Private 6G aims to leverage advanced technologies such as artificial intelligence (AI), machine learning (ML), and edge computing to deliver ultra-reliable, low-latency communication. The goal is to provide a network that can dynamically adapt to changing conditions, optimize resource allocation, and ensure high levels of security and privacy [154].

8.3.2. Key features and capabilities of private 6G

Private 6G networks are expected to introduce several groundbreaking features and capabilities. Dynamic spectrum sharing will allow for efficient allocation of spectrum resources, adapting to varying levels of demand and minimizing interference [155]. Ultra-high capacity and speed will support data rates up to 1 terabit per second (Tbps), enabling applications such as real-time 8K video streaming and holographic communications. The use of sub-terahertz (THz) frequency bands will achieve higher bandwidth and lower latency, essential for applications like autonomous driving and remote robotic surgery [156].

AI-driven network management will play a crucial role, enabling predictive maintenance, dynamic resource allocation, and real-time optimization of network performance [157]. Ultra-low latency, targeting levels below 1 millisecond, will benefit mission-critical applications such as industrial automation and remote healthcare. Massive device connectivity will support billions of devices, facilitating the proliferation of IoT and smart environments. Enhanced security measures, incorporating AI-driven protocols, will protect sensitive data and ensure user privacy. Seamless integration with edge computing will enable real-time data processing and analytics closer to the source, reducing latency and improving efficiency [158]. Finally, private 6G networks will focus on energy efficiency, incorporating technologies to reduce the overall carbon footprint.

8.3.3. Integration with enhanced spectrum utilization

The successful deployment of private 6G networks will rely heavily on enhanced spectrum utilization. Advanced spectrum sharing models will allow for dynamic and efficient allocation of spectrum resources, enabling multiple users to coexist on the same frequency bands without causing interference [155]. Collaborative spectrum management, involving industry stakeholders, government agencies, and academia, will facilitate the creation of a robust spectrum management framework. Effective regulatory frameworks will address issues related to spectrum allocation, interference management, and cross-border spectrum coordination [158].

Technological innovations such as intelligent spectrum sensing, cognitive radio, and dynamic spectrum access will enhance the capabilities of private 6G networks, allowing them to adapt to changing conditions and optimize spectrum usage in real-time. Spectrum aggregation techniques will combine multiple frequency bands to increase available bandwidth and improve network performance. AI-enhanced spectrum management will utilize AI and ML algorithms to predict spectrum demand, optimize allocation, and mitigate interference, ensuring that the network can meet the demands of diverse applications [155].

8.3.4. Expected benefits of private 6G networks

The implementation of private 6G networks will bring significant benefits across various sectors, enabling advanced manufacturing, telemedicine, smart cities, and autonomous transportation [159]. The ultra-reliable, low-latency communication capabilities of private 6G will be ideal for mission-critical operations, ensuring seamless and uninterrupted connectivity for applications such as emergency response and industrial automation. Enhanced user experience will be achieved through high capacity, low latency, and advanced features, improving applications such as immersive virtual reality, augmented reality, and high-definition video streaming. Additionally, the deployment of private 6G networks will drive economic growth by enabling new business models, creating job opportunities, and enhancing the competitiveness of enterprises.

6G networks are expected to offer robust security measures, personalized user experiences through AI, and extended capabilities of existing 5G applications. They will also drive the development of wireless sensing technologies, inspire new technological innovations, reduce costs through virtualization, improve cellular network penetration, and optimize indoor network usage [159].

Table 8 provides a detailed overview of the expected characteristics and features of private 6G networks, highlighting the advancements that will support diverse and demanding applications. The combination of enhanced security, personalization, extended application capabilities, advanced wireless sensing, and innovative technological developments will ensure that private 6G networks can meet the varied and demanding requirements of modern enterprises, driving the next wave of digital transformation across industries. The collaborative efforts of industry stakeholders, government agencies, and academia will be essential in realizing the full potential of private 6G networks and driving the digital transformation of various industries.

Table 8
Expected characteristics of private 6G networks.

Feature/Aspect	Private 6G networks
Spectrum coordination	Dynamic spectrum sharing, High availability
Coverage	Customizable, High transmit power, Sub-THz Bands
Latency	<1 ms
Security	Ultra-High with AI-driven security protocols
Capacity	Up to 1 Tbps
Scalability	Billions of devices
Control	High (enterprise-controlled)
Reliability	99.9999%
Customization	Extremely high
Use case suitability	Industry-specific, mission-critical applications
Cost	High initial investment, high long-term cost
Traffic handling	Intelligent scheduling, AI-Optimized traffic
Quality of service	Deterministic, AI-Enhanced RF feedback loop
Density handling	Multi-Factor OFDMA, AI-Managed interference
Mobility	Seamless Handoffs, AI-Optimized roaming

8.3.5. Spectrum considerations for private 6G

The evolution toward 6G will require a comprehensive approach to spectrum utilization, involving both new frequency bands and advanced techniques to optimize performance. The spectrum requirements for 6G will build upon and expand the capabilities established by 5G, enhancing features such as URLLCeMBB, massive machine-type communications (mMTC), and URLLC while introducing new dimensions in reliability, positioning, sensing accuracy, and energy efficiency [156,158].

- **Spectrum Bands for 6G:** 6G networks will operate across a multi-layered spectrum grid that includes low, mid, and high-frequency bands. Low and mid-band frequencies (below 6 GHz) will continue to provide broad coverage and capacity, essential for wide-area network deployment and ubiquitous connectivity [156]. New mid-band spectrum within the 7–15 GHz range, specifically from 7.125–8.5 GHz, 10.7–13.25 GHz, and 14–15.35 GHz, is crucial for balancing capacity and coverage, enabling efficient deployment and cost-effective operations [156]. High-frequency bands, such as sub-terahertz (sub-THz) spectrum (90–300 GHz), will offer extremely high data rates and wide bandwidths, essential for applications demanding high capacity and low latency, such as high-resolution holographic communication and advanced industrial automation [158].
- **Spectrum Aggregation and Management:** Efficient spectrum utilization in 6G will require advanced aggregation and management techniques. Dynamic spectrum sharing will enable the coexistence of different network generations, allowing 6G networks to utilize existing spectrum resources alongside new allocations. This approach will be essential for managing the increasing data traffic and ensuring seamless service continuity across different network layers. Spectrum aggregation techniques will combine multiple frequency bands to enhance overall bandwidth and improve network performance, involving both carrier aggregation and dual connectivity [158].
- **Regulatory Considerations and Global Harmonization:** The successful implementation of 6G will depend on timely regulatory decisions and global harmonization of spectrum bands. The International Telecommunication Union (ITU) and national regulatory bodies will play crucial roles in defining the spectrum roadmap for 6G. Decisions on candidate bands and usage conditions need to be made well in advance to ensure that the necessary spectrum is available for 6G deployment by the end of this decade [156]. Global harmonization of 6G frequency ranges and technical specifications will be critical for enabling worldwide interoperability, service continuity, and economies of scale. The ITU's World Radiocommunication Conferences (WRC) will be pivotal in this process, setting the stage for international agreements on 6G spectrum allocations [158].

These spectrum bands will be essential for 6G, especially in private networks, due to their coverage, capacity, and performance enhancements. Low and mid-band frequencies (below 6 GHz) provide broad coverage and capacity, crucial for wide-area deployment and ubiquitous connectivity. The mid-band spectrum (1–6 GHz) balances capacity and coverage, supporting efficient and cost-effective operations. High-frequency bands, such as the mmWave spectrum (above 6 GHz) and sub-terahertz spectrum (90–300 GHz), offer extremely high data rates and low latency, making them ideal for advanced industrial automation and high-resolution holographic communication, meeting the diverse needs of private 6G networks.

Table 9 summarizes the different spectrum bands that can be utilized in 6G networks and their respective applications, demonstrating that the High-Frequency spectrum band is the most suitable for Private 6G networks.

8.3.6. Architectural considerations for private 6G

Cagenius et al. advocate for early alignment on key architectural principles for 6G to ensure a smooth introduction and early monetization. Their vision includes a single-step migration to a standalone 6G radio-access technology available on all necessary spectrum bands, connected to an evolved 5G Core network. The architecture focuses on interfaces, network functions, and services relevant for multi-vendor deployments, ensuring openness and facilitating rapid standardization. Significant technology trends impacting 6G include monetization and exposure enablers, automation of network operations, cloud-native design, and network architecture evolution. Ericsson's proposal emphasizes the importance of dynamic spectrum sharing, horizontal separation of network functions, and enhanced RAN and core network architectures to support new use cases and service requirements for 2030 and beyond. The 6G architecture will build on the existing 5GC, aiming for efficiency, flexibility, and automation, while addressing energy performance and sustainability concerns. Early industry alignment will simplify the 6G introduction, reduce complexity, and enable service providers to capitalize on 6G capabilities from day one [160].

- Monetization and Exposure Enablers: Reuse and expand 5G capabilities for 6G.
- Automation of Network Operations: Utilize AI/ML for managing and optimizing networks.
- Cloud-Native Design: Implement containerized deployments to separate software from hardware.
- Network Architecture Evolution: Focus on migration, spectrum aggregation, and evolution of RAN and core network architectures.

Early alignment on 6G architecture will ease the transition from 5G, enhancing performance, flexibility, and automation, while reducing complexity and supporting early monetization [160]. Advanced

Table 9
Spectrum bands and their applications in 6G networks.

Spectrum band	Applications and benefits
Low band (Below 1 GHz)	Broad coverage, capacity for wide-area network deployment, ubiquitous connectivity [156]
Mid-band (1–6 GHz)	Balancing capacity and coverage, efficient deployment, cost-effective operations [156]
High-frequency (mmWave, Above 6 GHz, and Sub-Terahertz, 90–300 GHz)	Extremely high data rates, wide bandwidths, applications demanding high capacity and low latency, such as high-resolution holographic communication and advanced industrial automation [158]

spectrum use and flexible architecture will enable private 6G networks to meet diverse enterprise needs, offering superior performance, reliability, and adaptability for digital transformation. The future of private networks centers on private 6G, which promises unmatched performance, security, and spectrum efficiency. Industry, government, and academia must collaborate to unlock its full potential and drive digital transformation across sectors.

9. Conclusion and future work

The evolution of private networks from 4G/LTE to 5G has significantly enhanced their capabilities, addressing the increasing demands of modern industries. Private 5G networks offer substantial improvements in bandwidth, speed, and capacity, enabling advanced applications in manufacturing, healthcare, public safety, agriculture, and other sectors. The integration of private networks with spectrum sharing ensures efficient frequency use and optimal performance in high-demand environments. We highlight the superior performance of private 5G over traditional Wi-Fi and MNO networks, particularly in terms of latency, reliability, and scalability.

The future of private networks lies in the development of private 6G networks and next-generation spectrum technologies. These advancements promise to deliver ultra-reliable, low-latency communication, massive device connectivity, and enhanced security measures, supporting a wide range of industrial and commercial applications. Collaborative efforts among industry stakeholders, government agencies, and academia will be crucial in achieving these goals and ensuring that private networks continue to drive innovation and operational excellence across sectors. Future work in the domain of private networks should focus on several key areas to fully realize their potential:

- **Spectrum Sharing Models:** Ongoing research and development are needed to refine spectrum sharing models and ensure efficient spectrum utilization. This includes exploring advanced spectrum aggregation techniques and dynamic spectrum access methods.
- **Private 6G Networks:** The deployment and standardization of private 6G networks will require significant efforts in both technological innovation and regulatory alignment. Investigating the integration of AI-driven network management and edge computing will be essential to optimize performance and reduce latency.
- **Economic and Environmental Impacts:** Further studies should explore the economic and environmental impacts of private networks, particularly in the context of sustainable development and cost-effective deployment strategies.
- **Real-World Implementations:** Real-world implementations and pilot projects across diverse industries will provide valuable insights into the practical challenges and benefits of private networks.
- **Security and Privacy:** Addressing security and privacy concerns through advanced encryption methods and robust network protocols will be critical to ensuring the widespread adoption and trust in private network solutions.
- **Interoperability and Standards:** Development of global standards and ensuring interoperability between different private network deployments will be essential for the seamless integration of new technologies.
- **User Experience:** Enhancing user experience by focusing on low-latency, high-reliability, and secure communication for mission-critical applications.
- **Integration with Emerging Technologies:** Exploring the integration of private networks with emerging technologies such as IoT, AI, and edge computing to create more intelligent and responsive network environments.

Through these focused efforts, the future of private networks can be shaped to meet the evolving needs of a highly connected world. The advancements in spectrum utilization, network architectures, and security measures will ensure that private networks continue to drive innovation, efficiency, and productivity across various sectors.

CRediT authorship contribution statement

Onur Sahin: Writing – review & editing, Writing – original draft, Visualization, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Vanlin Sathya:** Validation, Supervision. **Mehmet Yavuz:** Project administration.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] Federal Communications Commission, 3.5 GHz band overview, 2015, Available: https://www.fcc.gov/wireless/bureau-divisions/mobility-division/35-ghz-band/35-ghz-band-overview.
[2] Wireless Innovation Forum, Citizens Broadband Radio Service (CBRS), Available: https://cbrs.wirelessinnovation.org.
[3] P. Marsch, 5G System Design: Architectural and Functional Considerations and Long Term Research, Wiley, 2018.
[4] S. Chen, S. Sun, G. Xu, X. Su, Y. Cai, Beam-space multiplexing: Practice, theory, and trends, from 4G TD-LTE, 5G, to 6G and beyond, IEEE Wirel. Commun. 27 (2) (2020) 162–172, http://dx.doi.org/10.1109/MWC.001.1900307.
[5] M. Ergen, Mobile Broadband: Including WiMAX and LTE, Springer, 2009.
[6] H. Holma, A. Toskala, LTE for UMTS: Evolution To LTE-Advanced, Wiley, 2011.
[7] Nisha Panwar, Shantanu Sharma, Awadhesh Kumar Singh, A survey on 5G: The next generation of mobile communication, Phys. Commun. (ISSN: 1874-4907) 18 (Part 2) (2016) 64–84, http://dx.doi.org/10.1016/j.phycom.2015.10.006.
[8] Allied Vision, Industrial cameras for industrial inspection and automation, allied vision, 2024, Available: https://www.alliedvision.com/en/applications/industrial-inspection-and-automation.
[9] E-Con Systems, Industrial cameras for visual inspection systems, E-Con systems, 2024, Available: https://www.e-consystems.com/markets/industrial-cameras/quality-control-inspection.asp.
[10] P. Nooralishahi, C. Ibarra-Castanedo, S. Deane, F. López, S. Pant, M. Genest, N.P. Avdelidis, X.P.V. Maldague, Drone-based non-destructive inspection of industrial sites: A review and case studies, Drones 5 (2021) 106, http://dx.doi.org/10.3390/drones5040106.
[11] Devdiscourse News Desk, 5G and telemedicine: Enabling next-generation healthcare services, devdiscourse, 2024, Available: https://www.hst.org.tw/en/story/content/4530.

[12] A.O. Adejo, A.J. Onumanyi, E.E. Ohihoin, A.I. Balarabe, S.A. Okoh, E. Kolo, Telemedicine: A survey of telecommunication technologies, developments, and challenges, J. Sens. Actuator Netw. 12 (2) (2023) 20, Available: DOI: 10.3390/jsan12020020.

[13] Medium, The Evolution of Telehealth: From Video Calls to AI-driven Selfie Diagnoses, Medium, 2024, Available: https://medium.com/docme-tech/the-evolution-of-telehealth-from-video-calls-to-ai-driven-selfie-diagnoses-24105606167b.

[14] M. Attaran, The impact of 5G on the evolution of intelligent automation and industry digitization, J. Ambient. Intell. Humaniz. Comput. 14 (2023) 5977–5993, http://dx.doi.org/10.1007/s12652-020-02521-x.

[15] G. Brown, Private 5G mobile networks for industrial IoT, heavy reading white paper produced for qualcomm, 2019, [Online]. Available: https://theinternetofthings.report/Resources/Whitepapers/6f44de77-8426-48b1-b858-0f8c6fa7b648_private-5g-networks-for-industrial-iot.pdf.

[16] Private industrial 5G networks (no date) siemens.com Global Website. Available at: https://www.siemens.com/global/en/products/automation/industrial-communication/industrial-5g/private-5g-networks-infrastructure.html.

[17] Private 5G networks for industrial IOT 2020. Advantech. Available at: https://www.advantech.com/en/resources/solution-brief/private-5g-networks-for-industrial-iot.

[18] 5G in Manufacturing: The Future of Factories (no date), Celona, Available at: https://www.celona.io/5g-lan/5g-in-manufacturing.

[19] The future of healthcare with Private 5G Networks (no date) Accelleran. Available at: https://accelleran.com/private-5g-networks-in-healthcare/.

[20] H. de Oliveira Lima, L.M. da Silva, A. de Campos Vieira Abib, et al., Coronavirus disease-related in-hospital mortality: a cohort study in a private healthcare network in Brazil, Sci. Rep. 12 (2022) 6371, http://dx.doi.org/10.1038/s41598-022-10343-4.

[21] First Ever Private 5G Network At an Operating European Hospital, Boldyn, 2024, Available at: https://www.boldyn.com/news/hola-5g-oulu-project.

[22] CJ logistics sees productivity surge with private 5G, 2023, Available at: https://www.ericsson.com/en/news/2023/12/cj-logistics-5g-enterprise.

[23] A. Navaneeth, How Private 5G Is Reshaping the Future of Logistics, HFCL, 2023, Available at: https://www.hfcl.com/blog/private-5G-in-logistics#:~:text=Private%205G%20in%20logistics%20has,risk%20of%20errors%20or%20delays.

[24] V. Capocasale, D. Gotta, S. Musso, G. Perboli, A blockchain, 5G and IoT-based transaction management system for smart logistics: an hyperledger framework, in: 2021 IEEE 45th Annual Computers, Software, and Applications Conference, COMPSAC, Madrid, Spain, 2021, pp. 1285–1290, http://dx.doi.org/10.1109/COMPSAC51774.2021.00179.

[25] C. Cheng, Application of 5G private network and internet of things in smart cold chain logistics park, in: 2022 IEEE Conference on Telecommunications, Optics and Computer Science, TOCS, Dalian, China, 2022, pp. 277–281, http://dx.doi.org/10.1109/TOCS56154.2022.10016203.

[26] M. Liu, Research on the development of intelligent logistics based on 5G technology, in: 2021 2nd International Conference on Urban Engineering and Management Science, ICUEMS, Sanya, China, 2021, pp. 107–110, http://dx.doi.org/10.1109/ICUEMS52408.2021.00029.

[27] Z. Yang, R. Wang, D. Wu, H. Wang, H. Song, X. Ma, Local trajectory privacy protection in 5G enabled industrial intelligent logistics, IEEE Trans. Ind. Inform. 18 (4) (2022) 2868–2876, http://dx.doi.org/10.1109/TII.2021.3116529.

[28] Sivaraman Eswaran, Prasad Honnavalli, Private 5G networks: a survey on enabling technologies, deployment models, use cases and research directions, Telecommun. Syst. 82 (2022) http://dx.doi.org/10.1007/s11235-022-00978-z.

[29] Christina Gericke, The global education industry in a microcosm: Public- private networks in german public schooling, J. Educ. Policy 37 (2021) 1–20, http://dx.doi.org/10.1080/02680939.2021.1915501.

[30] S. Bhaskaran, Private 5G: What Is It? how Does Itwork?, 5G Technology World, 2022, https://www.5gtechnologyworld.com/private-5g-what-is-it-how-does-it-work/.

[31] C. Bektas, S. Böcker, B. Sliwa, C. Wietfeld, Rapid network planning of temporary private 5G networks with unsupervised machine learning, in: 2021 IEEE 94th Vehicular Technology Conference, VTC2021-Fall, Norman, OK, USA, 2021, pp. 01–06, http://dx.doi.org/10.1109/VTC2021-Fall52928.2021.9625210.

[32] D. Kim, et al., Design and implementation of traffic generation model and spectrum requirement calculator for private 5G network, IEEE Access 10 (2022) 15978–15993, http://dx.doi.org/10.1109/ACCESS.2022.3149050.

[33] C. Bektas, C. Schüler, R. Falkenberg, P. Gorczak, S. Böcker, C. Wietfeld, On the benefits of demand-based planning and configuration of private 5G networks, in: 2021 IEEE Vehicular Networking Conference, VNC, Ulm, Germany, 2021, pp. 158–161, http://dx.doi.org/10.1109/VNC52810.2021.9644659.

[34] B. Mallikarjun, S. Sachinkumar, C. Schellenberger, C. Hobelsberger, H. Schotten, Performance analysis of a private 5G SA campus network, 2023.

[35] E. Calvanese Strinati, et al., Beyond 5G private networks: the 5G CONNI perspective, in: 2020 IEEE Globecom Workshops, GC Wkshps, 2020, pp. 1–6, http://dx.doi.org/10.1109/GCWkshps50303.2020.9367460.

[36] A. Aijaz, Private 5G: The future of industrial wireless, IEEE Ind. Electron. Mag. 14 (4) (2020) 136–145, http://dx.doi.org/10.1109/MIE.2020.3004975.

[37] Angin Pelin, Manolya Atalay, Fatma Gökçe, Ilsun You, A survey on the security of European 5G private networks, Res. Briefs Inf. Commun. Technol. Evol. 8 (2022) 162–181, http://dx.doi.org/10.56801/rebicte.v8i.149.

[38] M. Wen, et al., Private 5G networks: Concepts, architectures, and research landscape, IEEE J. Sel. Top. Signal Process. 16 (1) (2022) 7–25, http://dx.doi.org/10.1109/JSTSP.2021.3137669.

[39] H. Wang, R. Jain, A survey of private 5G, a survey of private 5G, 2022, Available at: https://www.cse.wustl.edu/jain/cse574-22/ftp/p5g/index.html.

[40] J. Prados-Garzon, P. Ameigeiras, J. Ordonez-Lucena, P. Muñoz, O. Adamuz-Hinojosa, D. Camps-Mur, 5G non-public networks: Standardization, architectures and challenges, IEEE Access 9 (2021) 153893–153908, http://dx.doi.org/10.1109/ACCESS.2021.3127482.

[41] M. Maman, E. Calvanese-Strinati, L.N. Dinh, et al., Beyond private 5G networks: applications, architectures, operator models and technological enablers, J. Wirel. Comed. Netw. 2021 (2021) 195, http://dx.doi.org/10.1186/s13638-021-02067-2.

[42] M.N. Patwary, S. Junaid Nawaz, M.A. Rahman, S.K. Sharma, M.M. Rashid, S.J. Barnes, The potential short- and long-term disruptions and transformative impacts of 5G and beyond wireless networks: Lessons learnt from the development of a 5G testbed environment, IEEE Access 8 (2020) 11352–11379, http://dx.doi.org/10.1109/ACCESS.2020.2964673.

[43] P. Scalise, M. Hempel, H. Sharif, A survey of 5G core network user identity protections, concerns, and proposed enhancements for future 6G technologies, Futur. Internet 17 (2025) 142, http://dx.doi.org/10.3390/fi17040142.

[44] A. Tusha, S. Dogan-Tusha, H. Nasiri, M.I. Rochman, P. McGuire, M. Ghosh, A comprehensive analysis of secondary coexistence in a real-world CBRS deployment, 2024, http://dx.doi.org/10.48550/arXiv.2402.05226, arXiv preprint arXiv:2402.05226. Retrieved from https://doi.org/10.48550/arXiv.2402.05226.

[45] W. Gao, A. Sahoo, Performance study of a GAA-GAA coexistence scheme in the CBRS band, in: 2019 IEEE International Symposium on Dynamic Spectrum Access Networks, DySPAN, Newark, NJ, USA, 2019, pp. 1–10, http://dx.doi.org/10.1109/DySPAN.2019.8935678.

[46] N. Jai, et al., Optimal channel allocation in the CBRS band with shipborne radar incumbents, in: 2021 IEEE International Symposium on Dynamic Spectrum Access Networks, DySPAN, Los Angeles, CA, USA, 2021, pp. 80–88, http://dx.doi.org/10.1109/DySPAN53946.2021.9677308.

[47] R. Berry, T. Hazlett, M.L. Honig, J. Laneman, Evaluating the CBRS experiment, SSRN Electron. J. (2023) http://dx.doi.org/10.2139/ssrn.4528763.

[48] P. Agarwal, M. Manekiya, T. Ahmad, A. Yadav, A. Kumar, M. Donelli, S.T. Mishra, A survey on citizens broadband radio service (CBRS), Electronics 11 (23) (2022) 3985, http://dx.doi.org/10.3390/electronics11233985.

[49] A. Ghosh, R. Berry, Entry and investment in CBRS shared spectrum, in: 2020 18th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, WiOPT, Volos, Greece, 2020, pp. 1–8.

[50] D.H. Kang, K. Balachandran, M. Buchmayer, Coexistence performance of GAA use cases using LTE-TDD technologies in 3.5 GHz CBRS spectrum, in: 2018 IEEE International Symposium on Dynamic Spectrum Access Networks, DySPAN, Seoul, Korea (South), 2018, pp. 1–7, http://dx.doi.org/10.1109/DySPAN.2018.8610475.

[51] W. Gao, A. Sahoo, Performance impact of coexistence groups in a GAA-GAA coexistence scheme in the CBRS band, IEEE Trans. Cogn. Commun. Netw. 7 (1) (2020) http://dx.doi.org/10.1109/tccn.2020.3003027.

[52] W. Gao, A. Sahoo, E. Bradford, GAA-GAA coexistence in the CBRS band: Performance evaluation of approach 3, in: 2020 IEEE 45th LCN Symposium on Emerging Topics in Networking, LCN Symposium, Sydney, Australia, 2020, pp. 39–47, http://dx.doi.org/10.1109/LCNSymposium50271.2020.9363267.

[53] A. Hikmaturokhman, K. Ramli, M. Suryanegara, A.A.P. Ratna, I.K. Rohman, M. Zaber, A proposal for formulating a spectrum usage fee for 5G private networks in Indonesian industrial areas, Informatics 9 (2) (2022) http://dx.doi.org/10.3390/informatics9020044.

[54] S. Guo, B. Lu, M. Wen, S. Dang, N. Saeed, Customized 5G and beyond private networks with integrated URLLC, eMBB, mMTC, and positioning for industrial verticals, IEEE Commun. Stand. Mag. 6 (1) (2022) 52–57, http://dx.doi.org/10.1109/MCOMSTD.0001.2100041.

[55] R. Bajracharya, R. Shrestha, H. Jung, Future is unlicensed: Private 5G unlicensed network for connecting industries of future, Sens. (Basel) 20 (10) (2020) 2774, http://dx.doi.org/10.3390/s20102774.

[56] A. Chakraborty, R.R. Rao, On Temporal and Spatial Behaviors of CBRS SAS, in IEEE Transactions on Cognitive Communications and Networking, doi: http://dx.doi.org/10.1109/TCCN.2024.3391331.

[57] L.P. Rachakonda, M. Siddula, V. Sathya, A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in next-generation networks (5G/6g/beyond), High-Confid. Comput. (2) (2024) 100220, http://dx.doi.org/10.1016/j.hcc.2024.100220.

[58] V. Sathya, A. Deshmukh, M. Shah, M. Yavuz, Battery life: Performance analysis and comparison between Wi-Fi, CBRS, and macro deployment system, in: 2024 International Conference on Computing, Networking and Communications, ICNC, Big Island, HI, USA, 2024, pp. 843–849.

[59] V. Sathya, L. Zhang, M. Yavuz, A comparative measurement study of commercial WLAN and 5G LAN systems, in: 2022 IEEE 96th Vehicular Technology Conference, VTC2022-Fall, London, United Kingdom, 2022, pp. 1–7, http://dx.doi.org/10.1109/VTC2022-Fall57202.2022.10013019.

[60] V. Sathya, L. Zhang, M. Goyal, M. Yavuz, Warehouse deployment: A comparative measurement study of commercial Wi-Fi and CBRS systems, in: 2023 International Conference on Computing, Networking and Communications, ICNC, Honolulu, HI, USA, 2023, pp. 242–248, http://dx.doi.org/10.1109/ICNC57223.2023.10074584.

[61] V. Sathya, A. Deshmukh, M. Goyal, M. Yavuz, Roaming performance analysis and comparison between Wi-Fi and private cellular network, in: 2024 International Conference on Computing, Networking and Communications, ICNC, Big Island, HI, USA, 2024, pp. 944–950, http://dx.doi.org/10.1109/ICNC59896.2024.10556190.

[62] Mark, Private 5G internationally at WLPC prague, Marko does wireless, 2023, Available at: https://markhoutz.com/2022/11/15/private-5g-internationally-at-wlpc-prague.

[63] 3.5 Ghz Band Overview, Federal Communications Commission, 2023, Available at: https://www.fcc.gov/wireless/bureau-divisions/mobility-division/35-ghz-band/35-ghz-band-overview.

[64] Celona, 5G, Private Spectrum and CBRS, Celona.io. Available at: https://www.celona.io/cbrs/cbrs-5g.

[65] STL Partners, CBRS SAS players: Who are they and what do they do? STLPartners.com. Available at: https://stlpartners.com/articles/private-cellular/cbrs-sas/.

[66] RF Everything, 5G Frequency Spectrum in Mexico, Available at: https://www.everythingrf.com/community/5g-frequency-spectrum-in-mexico.

[67] CMS Law, 5G regulation and law in Mexico, available at: https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g-regulation-and-law/mexico#:~:text=There%20are%20no%20regulations%20on,provision%20of%20telecommunications%20and%20broadcasting.

[68] Innovation, Science and Economic Development Canada (ISED), Spectrum Management and Telecommunications, Available: https://ised-isde.canada.ca/site/spectrum-management-telecommunications/en.

[69] RCR Wireless News, Brazil raises a total of $8.5 billion in 5G spectrum auction, Available at: https://www.rcrwireless.com/20211108/5g/brazil-raises-total-8-billion-5g-spectrum-auction/amp.

[70] CMS Law, 5G regulation and law in Brazil, Available at: https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g-regulation-and-law/brazil.

[71] CMS Law, 5G regulation and law in Belgium, Available at: https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g-regulation-and-law/belgium.

[72] RCR Wireless News, Belgium's 5G spectrum auction raises $1.26 billion, Available at: https://www.rcrwireless.com/20220621/5g/belgium-5g-spectrum-auction-raises-1-billion.

[73] RCR Wireless News, Netherlands opens 3.6 GHz band for private 5G, Available at: https://www.rcrwireless.com/20231109/5g/netherlands-opens-3-6-ghz-band-for-private-5g.

[74] R. Orugu, N. Moses, D.K. Janapala, Frequency reconfigurable antenna for 5G applications at n77 and n78 bands, in: N. Gupta, P. Pareek, M. Reis (Eds.), Cognitive Computing and Cyber Physical Systems, IC4S 2022, in: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 472, Springer, Cham, 2023.

[75] Commission for Communications Regulation (ComReg), About 5G, Available at: https://www.comreg.ie/industry/radio-spectrum/about-5g/.

[76] Environmental Protection Agency (EPA), 5G in Ireland, Available at: https://www.epa.ie/environment-and-you/radiation/emf/what-is-emf/radiofrequency-fields-/5g—new-rf-technologies/5g-in-ireland/.

[77] Silicon Republic, Irish mobile operators pay €448 m in 5G spectrum auction, Available at: https://www.siliconrepublic.com/comms/ireland-5g-spectrum-band-auction-comreg#:~:text=Vodafone%2C%20Three%20and%20Eir%20are,448m%20in%20a%20spectrum%20auction.

[78] Digital Regulation Platform, Spectrum licensing: local and private networks in Germany, available at: https://digitalregulation.org/spectrum-licensing-local-and-private-networks-in-germany/#:~:text=In%20November%202019%2C%20Germany%20opened,in%20a%20defined%20coverage%20area.

[79] RCR Wireless News, German regulator has already approved 123 private 5G networks, available at: https://www.rcrwireless.com/20210607/5g/german-regulator-already-awarded-123-private-5g-networks#:~:text=German%20regulator%20has%20already%20approved%20123%20private%205G%20networks,-By%20Juan%20Pedro&text=The%20German%20federal%20network%20agency,3.8%20GHz%20for%20local%20networks.

[80] CMS Law, 5G regulation and law in Germany, Available at: https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g-regulation-and-law/germany.

[81] RCR Wireless News, Switzerland to release 3.4-3.5 GHz band for private 5G from 2024, Available at: https://www.rcrwireless.com/20230913/private-5g/switzerland-to-release-3-4-3-5-ghz-band-for-private-5g-from-2024.

[82] TelecomTalk, Switzerland to Open Private 5G Network Frequencies in 2024, Available at: https://telecomtalk.info/switzerland-open-private-5gnetwork-frequencies-starting-january2024/870752/.

[83] Federal Office of Communications (OFCOM), Mobile radio frequencies for 5G awarded in Switzerland, Available at: https://www.bakom.admin.ch/bakom/en/homepage/frequencies-and-antennas/award-of-mobile-telephony-frequencies/starting-signal-for-new-award-of-mobile-radio-frequencies.html.

[84] ARCEP, Available: https://en.arcep.fr.

[85] Everything RF, 5G Frequency Spectrum in China, Available at: https://www.everythingrf.com/community/5g-frequency-spectrum-in-china.

[86] X. Chen, Session 2-5.pdf - ITU, itu.int, 2018, Available at: https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/ConformityandInteroperability2018/Session%202-5.pdf.

[87] ResearchGate, Vertically Polarized Quasi-Yagi MIMO Antenna for 5G N78 Band Application, Available at: https://www.researchgate.net/publication/346246992_Vertically_Polarized_Quasi-Yagi_MIMO_Antenna_for_5G_N78_Band_Application.

[88] Everything RF, 5G Frequency Spectrum in Japan, Available at: https://www.everythingrf.com/community/5g-frequency-spectrum-in-japan.

[89] Halberd Bastion, n79 (4500 MHz), Available at: https://halberdbastion.com/technology/cellular/5g-nr/5g-frequency-bands/n79-4500-mhz.

[90] Xu Yi, Yuandan Dong, Si Wen, Hailong Wang, Vertically polarized quasi-yagi MIMO antenna for 5G N78 band application, IEEE Access (1) (2021) http://dx.doi.org/10.1109/ACCESS.2020.3049058.

[91] Everything RF, 5G Frequency Spectrum in South Korea, Available at: https://www.everythingrf.com/community/5g-frequency-spectrum-in-south-korea.

[92] Netmanias, The South Korean government's regulations on private 5G, Available at: https://www.netmanias.com.

[93] ScienceDirect, Why is South Korea at the forefront of 5G? Insights from technology, market, and policy perspectives, Available at: https://www.sciencedirect.com/science/article/pii/S0308596121001414.

[94] Australian communications and media authority (ACMA), 2023, https://www.acma.gov.au/how-we-plan-and-manage-spectrum.

[95] L. Zhang, A. Ijaz, P. Xiao, A. Quddus, R. Tafazolli, Subband filtered multi-carrier systems for multi-service wireless communications, IEEE Trans. Wirel. Commun. 16 (3) (2017) 1893–1907, http://dx.doi.org/10.1109/TWC.2017.2656904.

[96] C. Cano, D.J. Leith, A. Garcia-Saavedra, P. Serrano, Fair coexistence of scheduled and random access wireless networks: Unlicensed LTE/WiFi, IEEE/ACM Trans. Netw. 25 (6) (2017) 3267–3281, http://dx.doi.org/10.1109/TNET.2017.2731377.

[97] A. Mukherjee, et al., Licensed-assisted access LTE: coexistence with IEEE 802.11 and the evolution toward 5G, IEEE Commun. Mag. 54 (6) (2016) 50–57, http://dx.doi.org/10.1109/MCOM.2016.7497766.

[98] Y. Jiang, J. Guo, Z. Fei, Performance analysis of the coexistence of 5G NR-unlicensed and Wi-Fi with mode selection, in: 2020 IEEE/CIC International Conference on Communications in China, ICCC, Chongqing, China, 2020, pp. 953–958, http://dx.doi.org/10.1109/ICCC49849.2020.9238800.

[99] A.M. Cavalcante, et al., Performance evaluation of LTE and Wi-Fi coexistence in unlicensed bands, in: 2013 IEEE 77th Vehicular Technology Conference, VTC Spring, Dresden, Germany, 2013, pp. 1–6, http://dx.doi.org/10.1109/VTCSpring.2013.6692702.

[100] Shinde Bhausaheb, V. Vijayabaskar, Analysis of LTE and Wi-Fi coexistence in 5 GHz unlicensed band, 2020.

[101] Noryusra Rosele, Khuzairi Mohd Zaini, Nurakmal Ahmad Mustaffa, Ahmad Abrar, Suzi Iryanti Fadilah, Mohammed Madi, Digital transformation in wireless networks: A comprehensive analysis of mobile data offloading techniques, challenges, and future prospects, J. King Saud Univ. - Comput. Inf. Sci. (ISSN: 1319-1578) 36 (5) (2024) 102071, http://dx.doi.org/10.1016/j.jksuci.2024.102071.

[102] MarchNet, Private LTE for advanced connectivity, 2023, [Online]. Available: https://marchnet.com.au/2024/04/03/unlocking-private-lte-for-advanced-connectivity/.

[103] Ruckus Networks, Private LTE for Higher Education. [Online]. Available: https://webresources.ruckuswireless.com/pdf/appnotes/appnote-private-lte.pdf.

[104] I. Shostko, A. Tevyashev, O. Zemlyaniy, Y. Kulia, Introduction of private LTE networks to provide specific communication tasks in various spheres of society and the state, in: 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology, PIC S & T, Kharkiv, Ukraine, 2021, pp. 583–586, http://dx.doi.org/10.1109/PICST54195.2021.9772142.

[105] Ericsson, Non-standalone and standalone: two paths to 5G, 2023, [Online]. Available: https://www.ericsson.com/en/blog/2023/4/standalone-and-non-standalone-5g-nr-two-5g-tracks.

[106] 5G NSA Vs 5G SA | What are the Differences Between NSA 5G and Standalone 5G Deployments? | Corning, Corning, Available at: https://www.corning.com/optical-communications/worldwide/en/home/the-signal-network-blog/5g-sa-vs-nsa.html.

[107] G. Fettweis, S. Alamouti, 5G: Personal mobile internet beyond what cellular did to telephony, IEEE Commun. Mag. 52 (2) (2014) 140–145, http://dx.doi.org/10.1109/MCOM.2014.6736754.

[108] J.G. Andrews, et al., What will 5G Be? IEEE J. Sel. Areas Commun. 32 (6) (2014) 1065–1082, http://dx.doi.org/10.1109/JSAC.2014.2328098.

[109] V. Petrov, et al., Achieving end-to-end reliability of mission-critical traffic in softwarized 5G networks, IEEE J. Sel. Areas Commun. 36 (3) (2018) 485–501, http://dx.doi.org/10.1109/JSAC.2018.2815419.

[110] E. Dahlman, S. Parkvall, J. Skold, 5G NR: The Next Generation Wireless Access Technology, Academic Press, 2018.
[111] D. Wubben, et al., Benefits and impact of cloud computing on 5G signal processing: Flexible centralization through cloud-RAN, IEEE Signal Process. Mag. 31 (6) (2014) 35–44, http://dx.doi.org/10.1109/MSP.2014.2334952.
[112] Polese Michele, Federico Chiariotti, Elia Bonetto, Filippo Rigotto, Andrea Zanella, Michele Zorzi, A survey on recent advances in transport layer protocols, IEEE Commun. Surv. Tutor. (2019) 1, http://dx.doi.org/10.1109/COMST.2019.2932905.
[113] Polese Michele, Marco Giordani, Marco Mezzavilla, Sundeep Rangan, Michele Zorzi, Improved handover through dual connectivity in 5G mmwave mobile networks, IEEE J. Sel. Areas Commun. (2016) http://dx.doi.org/10.1109/JSAC.2017.2720338.
[114] S. Parkvall, E. Dahlman, A. Furuskar, M. Frenne, NR: The new 5G radio access technology, IEEE Commun. Stand. Mag. 1 (4) (2017) 24–30, http://dx.doi.org/10.1109/MCOMSTD.2017.1700042.
[115] X. Ge, H. Cheng, M. Guizani, T. Han, 5G wireless backhaul networks: challenges and research advances, IEEE Netw. 28 (6) (2014) 6–11, http://dx.doi.org/10.1109/MNET.2014.6963798.
[116] H. Ji, S. Park, J. Yeo, Y. Kim, J. Lee, B. Shim, Ultra-reliable and low-latency communications in 5G downlink: Physical layer aspects, IEEE Wirel. Commun. 25 (3) (2018) 124–130, http://dx.doi.org/10.1109/MWC.2018.1700294.
[117] CBRS and Wi-Fi: Which Is Best for Your Organization?, Celona, 2021, Available at: https://www.celona.io/cbrs/cbrs-vs-wifi#:~:text=Quality%20of%20Service&text=While%20Wi-Fi%20enables%20segmentation,through%20its%20unique%20MicroSlicing%20technology.
[118] Private LTE Vs. Wi-Fi for Enterprise: Comparison & Use Cases, Celona, 2021, Available at: https://www.celona.io/cbrs/private-lte-vs-wi-fi-for-enterprise-comparison-use-cases.
[119] L. Vosteen, F. John, J. Schuljak, B. Sievers, A. Hanemann, H. Hellbrueck, Practical security analysis and measures for 5G private industrial standalone (SA) deployments, in: Mobile Communication - Technologies and Applications; 26th ITG-Symposium, Osnabrueck, Germany, 2022, pp. 1–6.
[120] Chen Xingshu, Zeng Xuemei, Wenxian Wang, Guolin Shao, Big data analytics for network security and intelligence, Gongcheng Kexue Yu Jishu/Adv. Eng. Sci. 49 (2017) 1–12, http://dx.doi.org/10.15961/j.jsuese.201600352.
[121] Z. He, Q. Wu, Q. Zhang, Intelligent connectivity for 5G-enabled autonomous vehicles, IEEE Netw. 35 (4) (2021) 215–221.
[122] M. Gerla, E.K. Lee, G. Pau, U. Lee, Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds, in: 2014 IEEE World Forum on Internet of Things, WF-IoT, 2014, pp. 241–246.
[123] J. Palmer, Drones As First Responders – Enabled By Telco Cloud and 5G Autonomous Networks, IBM Blog, 2020, Available at: https://www.ibm.com/blog/drones-as-first-responders-enabled-by-telco-cloud-and-5g-autonomous-networks.
[124] J. Ferreira, M. Alam, B. Fernandes, L. Silva, J. Almeida, L. Moura, R. Costa, G. Iovino, E. Cordiviola, Cooperative sensing for improved traffic efficiency: the highway field trial, Comput. Netw. 143 (2018) 82–97.
[125] A. Gohar, G. Nencioni, The role of 5G technologies in a smart city: the case for intelligent transportation system, Sustainability 13 (9) (2021) 5188.
[126] W. Viriyasitavat, A.A. Alghamdi, Intelligent transportation using wireless sensor networks, blockchain, and license plate recognition, Sensors 23 (5) (2023) 2670.
[127] Aalsalem Mohammed, Wazir Khan, Wajeb Gharibi, Khurram Khan, Quratulain Arshad, Wireless sensor networks in oil and gas industry: Recent advances, taxonomy, requirements, and open challenges, J. Netw. Comput. Appl. 113 (2018) http://dx.doi.org/10.1016/j.jnca.2018.04.004.
[128] Pan Yi, Xiao Lizhi, Zhang Yuanzhong, Remote Real-Time Monitoring System for Oil and Gas Well Based on Wireless Sensor Networks, Wuhan, China, 2010, pp. 2427–2429, http://dx.doi.org/10.1109/MACE.2010.5535870.
[129] Private LTE and 5G in Oil and Gas, and Mining Industry, Athonet, 2024, Available at: https://athonet.com/industries/mining-oil-and-gas.
[130] FutureIoT, The transformational potential of private 5G wireless networks, 2023, https://futureiot.tech/the-transformational-potential-of-private-5g-wireless-networks/.
[131] Inseego, Five benefits of 5G in retail environments, 2023, https://inseego.com/resources/blog/five-benefits-of-5g-in-retail-environments/.
[132] Telit, 5G use cases in retail and consumer technology, 2023, https://www.telit.com/blog/5g-use-cases-retail/.
[133] K. Sprague, Developing Our Fulfillment Network for the Future, Walmart Corporate News and Information, 2022, Available at: https://corporate.walmart.com/news/2022/10/10/developing-our-fulfillment-network-for-the-future.
[134] Niral Networks, Private 5G: Transforming Airports Into Smart Airports, Niral Networks, 2024, Available at: https://niralnetworks.com/private-5g-transforming-airports-into-smart-airports.
[135] T. May, Europe's Largest Private 5G Network To Be Built At Frankfurt Airport, Airport Industry-News, 2022, https://airportindustry-news.com/europes-largest-private-5g-network-to-be-built-at-frankfurt-airport/.
[136] Building a Private 5G Network To Support Smart Warehouse Applications, Deloitte, https://www2.deloitte.com/content/dam/Deloitte/br/Documents/energy-resources/us-deloitte-building-5G-private-network.pdf.
[137] Powering Warehousing and Logistics with Seamless 5G Connectivity, Ericsson, https://www.ericsson.com/en/industries/warehousing-and-logistics.
[138] Niral Networks, Private 5G: Transforming healthcare, 2022, https://niralnetworks.com/private-5g-transforming-healthcare/.
[139] Research (no date) EPFL. Available at:https://www.epfl.ch/schools/ic/research/.
[140] Port Economics, Management and Policy, Distribution networks, 2023, https://porteconomicsmanagement.org.
[141] Security for Public & Private Networks. TeckNexus. https://tecknexus.com/security/.
[142] J. Glascock, (no date) Top 10 cities for a distribution center in the U.S. Kenco. Available at: https://blog.kencogroup.com/top-10-cities-for-a-distribution-center.
[143] V.K. Sharma, T. Panagiotakopoulos, A. Kameas, Networking architectures and protocols for IoT applications in smart cities: Recent developments and perspectives, Electronics 12 (11) (2023) 2490, http://dx.doi.org/10.3390/electronics12112490.
[144] A. Hilmani, A. Maizate, L. Hassouni, Automated Real-Time Intelligent Traffic Control System for Smart Cities using Wireless Sensor Networks, vol. 19, RITM-ESTC/CED-ENSEM, University Hassan II, 2023, pp. 780–790, (6).
[145] Development of a National Spectrum Strategy Docket No. NTIA-2023-0003-0001, NTIA, 2023, Available at: https://www.ntia.gov/sites/default/files/2023-09/national_spectrum_consortium_written_input.pdf.
[146] Emilio, et al., Beyond 5G private networks: the 5G CONNI perspective, 2020, pp. 1–6, http://dx.doi.org/10.1109/GCWkshps50303.2020.9367460.
[147] P. Goldstein, DOD looks to spectrum sharing to support 5G efforts, Fedtechmagazine, 2023, Available at: https://fedtechmagazine.com/article/2022/08/dod-looks-spectrum-sharing-support-5g-efforts-perfcon.
[148] C.T. Lopez, Spectrum Sharing Is Way Ahead To Maintain Economic Dominance, Defense Official Says, U.S. Department of Defense, 2022, Available at: https://www.defense.gov/News/News-Stories/Article/Article/3165774/spectrum-sharing-is-way-ahead-to-maintain-economic-dominance-defense-official-s.
[149] Power, et al., Request for Information Regarding Next-Generation Electromagnetic Spectrum Strategic Roadmap, CTIA, 2023, Available at: https://api.ctia.org/wp-content/uploads/2023/02/230217-CTIA-White-Paper-on-DoD-Strategic-Spectrum-Roadmap-RFI.pdf.
[150] M. Alleven, DOD outlines spectrum moonshot endeavor during eclipse, fierce network, 2024, Available at: https://www.fierce-network.com/wireless/dod-outlines-spectrum-moonshot-plan-during-eclipse.
[151] D. Combs, DOD releases redacted report on possibility of sharing 3 ghz band, inside towers, 2024, Available at: https://insidetowers.com/dod-releases-redacted-report-on-possibility-of-sharing-3-ghz-band/.
[152] A. Keeney, National spectrum consortium launches PATHSS task group to explore 5G spectrum sharing, business wire, 2021, Available at: https://www.businesswire.com/news/home/20211027005267/en/National-Spectrum-Consortium-Launches-PATHSS-Task-Group-to-Explore-5G-Spectrum-Sharing.
[153] J. Gallagher, Repurposing 3.1-3.55 GHz spectrum: Issues for congress, sgp.fas.org, 2023, Available at: https://sgp.fas.org/crs/misc/IF12351.pdf.
[154] C.-X. Wang, et al., On the road to 6G: Visions, requirements, key technologies, and testbeds, IEEE Commun. Surv. Tutor. 25 (2) (2023) 905–974, http://dx.doi.org/10.1109/COMST.2023.3249835.
[155] Microsoft Research, 6G | space: New spectrum and sharing, microsoft, 2023, Available: https://www.microsoft.com/en-us/research/project/6g-space/articles/6g-space-new-spectrum-and-sharing.
[156] Spectrum for 6G Explained, Nokia, 2023, Available at: https://www.nokia.com/about-us/newsroom/articles/spectrum-for-6G-explained.
[157] E. Calvanese Strinati, et al., 6G: The next frontier: From holographic messaging to artificial intelligence using subterahertz and visible light communication, IEEE Veh. Technol. Mag. 14 (3) (2019) 42–50, http://dx.doi.org/10.1109/MVT.2019.2921162.
[158] 6G spectrum and the road to extreme performance (no date) Ericsson. Available at: https://www.ericsson.com/en/6g/spectrum.
[159] Chiradeep BasuMallick, What Is a 6G Network? Working and Benefits - Spiceworks, Spiceworks Inc., 2023, Available at: https://www.spiceworks.com/tech/networking/articles/what-is-6g/#_003.
[160] Cagenius, et al., 6G Network Architecture – a Proposal for Early Alignment - Ericsson, Ericsson, 2023, Available at: https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/6g-network-architecture. (Accessed 09 July 2024).