Master of Science in Internetworking

Department of Electrical and Computer Engineering

Project Title:

A Study of Private Wireless Networks, Use Cases and Challenges

Supervisor:

Shahnawaz Mir

Provided By:

Kehinde Balogun

Fall 2022 - Winter 2023

Table of Contents

List of Figures

List of Tables

List of Abbreviations

1G	First Generation
2G	Second Generation
3G	Third Generation
3GPP	3rd Generation Partnership Project
4G	Fourth Generation
5G	Fifth Generation
AF	Application Function
AGV	Automated Guided Vehicle
AI	Artificial Intelligence
AMF	Core Access and Mobility Management Function
AMPS	Advanced Mobile Phone System
API	Application Programming Interface
APOC	Airport Operations Center
AR	Augmented Reality
ATM	Asynchronous Transfer Mode
AuC	Authentication Center
AUSF	Authentication Server Function
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CBRS	Citizen Broadband Radio Services
CBSD	Citizen Broadband Radio Service Device
CDMA	Code Division Multiple Access
CIA	Confidentiality, Integrity, and Availability
CP	Cyclic Prefix
CSIS	Canada Security Intelligence Service
DCI	Downlink Control Information
DCS	Digital Cross-connect System

DFT-s-OFDM	Discrete Fourier Transform-spread-OFDM
DN	Data Network
DoD	Department of Defense
DS-WCDMA	Direct Sequence Wideband Code Division Multiple Access
EC	European Commission
ECG	Electrocardiogram
EDGE	Enhanced Data Rates for GSM Evolution
EIR	Equipment Identity Register
eMBB	Enhanced Mobile Broadband
eNodeB	Enhanced NodeB
EPC	Evolved Packet Core Network
ESC	Environmental Sensing Capabilities
ETSI	European Telecommunication Standards Institute
EUD	End User Device
E-UTRAN	Evolved-UMTS Terrestrial Radio Access Network
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
FDM	Frequency Division Multiplexing
FDMA	Frequency Division Multiple Access
FSS	Fixed Satellite Service
FWA	Fixed Wireless Access
GAA	General Authorized Access
GGSN	Gateway GPRS Support Node
GMSC	Gateway Mobile Switching Center
GMSK	Gaussian Minimum Shift Keying
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
GSN	GPRS Support Nodes
GUTI	Globally Unique Temporary Identity
HARQ	Hybrid Automatic Request

HLR	Home Location Register
HSDPA	High-Speed Downlink Packet Access
HSPA	High-Speed Packet Access
HSPA+	Evolved High-Speed Packet Access
HSS	Home Subscriber Server
HSUPA	High-Speed Uplink Packet Access
IA	Incumbent Access
IAM	Identity and Access Management
ICIC	Inter-Cell Interference Coordination
IDU	Indoor Unit
IMEI	International Equipment Identity Number
IMT-2000	International Mobile Telecommunication-2000
IoT	Internet of Things
ITU	International Telecommunication Union
IWF	Internetworking Function
LAN	Local Area Network
LPWA	Low Power Wide Area
LSA	Licensed Shared Access
LTE	Long Term Evolution
ME	Mobile Equipment
ME	Mobile Equipment
MIB	Master Information Block
MIMO	Multiple Input Multiple Output
MME	Mobility Management Element
MMS	Multimedia Messaging Service
mMTC	Massive Machine Type Communication
MNO	Mobile Network Operator
MR	Mixed Reality
MS	Mobile Station
MSC	Mobile Switching Center

MTSO	Mobile telephone system office MTSO
NIBP	Non-invasive Blood Pressure
NMS	Network Management System
NR	New Radio
NRA	National Regulatory Authority
NSSF	Network Slice Selection Function
OAM	Operation, Administration, and Maintenance
ODU	Outdoor Unit
OFDMA	Orthogonal Frequency Division Multiple Access
OML	Operation and Maintenance Link
PA	Priority Access
PBCH	Physical Broadcast Channel
PCAST	President's Council of Advisors on Science and Technology
PCF	Policy Control Function
PCM	Pulse Code Modulation
PCRF	Policy Control and Charging Rule Function
PCS	Personal Communications Services
PDCCH	Physical Downlink Control Channel
PDSCH	Physical Data Shared Channel
PGW	Packet Data Network Gateway
PRACH	Physical Random Access Channel
PSBN	Public Safety Broadband Network
PSTN	Public service telephone network
PSTN	Public Service Telephone Network
PUCCH	Physical Uplink Control Channel
PUSCH	Physical Uplink Shared Channel
QoS	Quality of Service
RAN	Radio Access Network
RBC	Radio Bearer Control
RCMP	Royal Canadian Mounted Police

RELP-LTP	Regular Excited Linear Prediction Long Term Prediction
RF	Radio Frequency
RMC	Radio Mobility Control
RNC	Radio Network Controller
RRM	Radio Resource Management
SAS	Spectrum Access System
SCCP	Signaling Connection Control Part
SC-FDMA	Single-Carrier Frequency Division Multiple Access
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SIM	Subscriber Identity Module
SMF	Session Management Function
SMS	Short Messaging Service
SON	Self-Organizing Network
TACS	Total Access Communication Services
TDD	Time Division Duplex
TDMA	Time Division Multiple Access
TRAU	Transcoding and Rate Adaptation Unit
TSP	Toolless Sensor Platform
UCI	Uplink Control Information
UDM	Unified Data Management
UE	User Equipment
UMTS	Universal Mobile Telecommunication System
UPF	User Plane Function
URLLC	Ultra-Reliable Low Latency Communication
USIM	UMTS Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Network
VLR	Visitor Location Register
VR	Virtual Reality
WAN	Wide Area Network

Abstract

Traditional cellular and wireless technologies met business and consumer expectations during the first few years of launch. Unfortunately, the rapid growth of wireless demand and internet connectivity in the 21st century has resulted in high bandwidth requirements and an equally proportional need for spectrum allocation. As enterprises become more autonomous and distributed, modern network devices and applications demand more spectrum, bandwidth, availability, reliability, and lower latency. Private wireless networks is a 3GPP-based standalone 5G networks that enterprises and governmental organizations can leverage to provide scalable services, make faster and better decisions and improve overall productivity.

This report gives a brief explanation of the history of cellular wireless technologies. This includes the components, architectures, benefits, and limitations of each technology. The recent 5G technology tends to solve the challenges faced by previous wireless technologies. This paper discusses the application of 5G technology in private wireless networks, use cases, and challenges. I have analyzed various research papers that analyzed how this solution can be implemented in various enterprises and governmental organizations in Canada. Nowadays, since more and more enterprises are moving into private 5G networks, it is necessary to deeply understand and research the application of private wireless networks in enterprises and governmental organizations.

Acknowledgment

Firstly, I would like to express my sincere gratitude to my project supervisor and program coordinator, Shahnawaz Mir, for his mentorship and supervision during this project. His constant support and expertise are invaluable and deeply appreciated.

Secondly, I would like to express my gratitude to my program director, Prof. Mike Macgregor, and also, to Sharon Gannon, for their prompt responsiveness and support during the program.

Thirdly, I would like to extend my sincere gratitude to the University of Alberta for giving me access to both physical and online library resources during this project.

Finally, I would like to express my gratitude to my wife and children for their support and encouragement during this program.

Chapter 1: Cellular Network Technologies

1.1 1G Cellular Technology

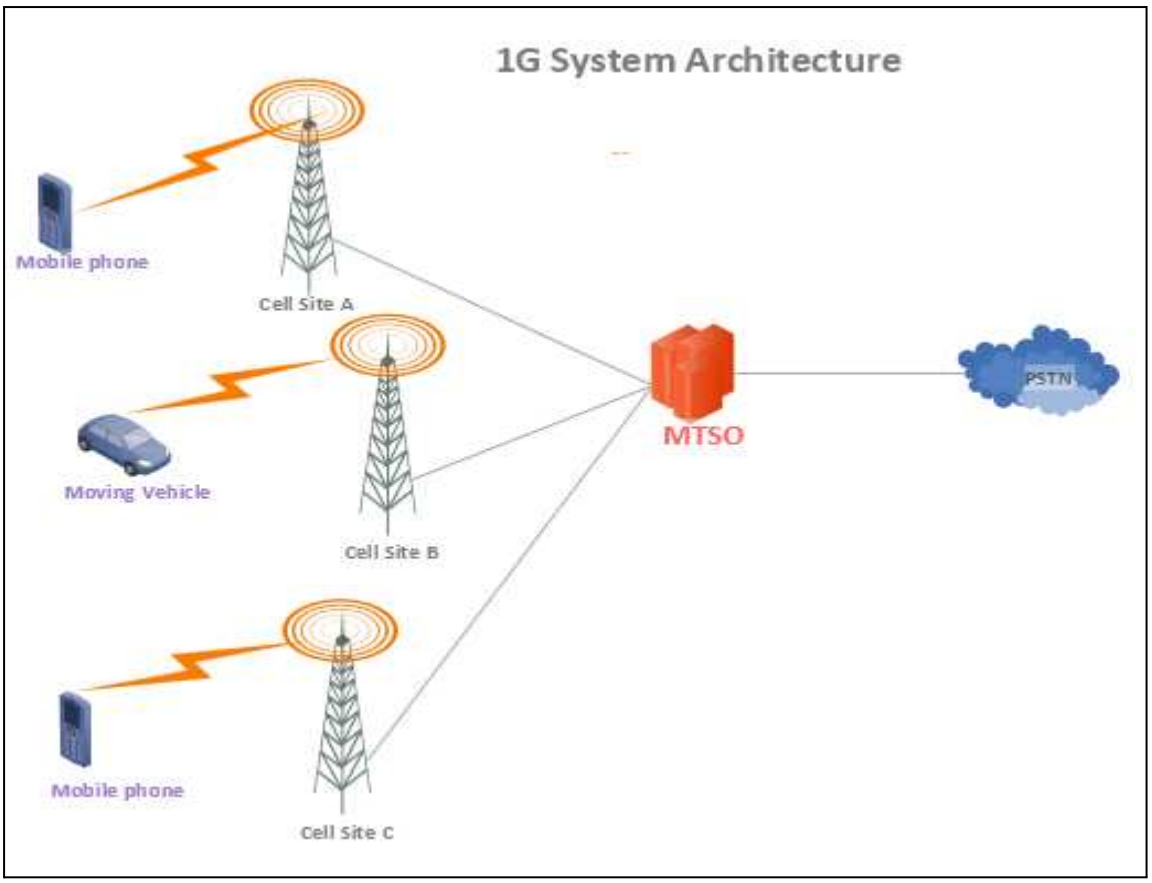
First Generation (1G) cellular network was the first cellular technology to employ frequency reuse for voice communication to support the mobility of the subscribers due to handoffs between base stations and accommodate more users in a geographic location. It was an analog-based system where the transfer of information between the mobile device and base stations did not involve CODEC. 1G technology utilizes the Frequency Division Multiple Access (FDMA) schemes for radio access. Its cellular concept was based on the Advanced Mobile Phone System (AMPS) or Total Access Communication Services (TACS) technology. AMPS operated in the 800MHz frequency band (Tx = 869 – 894 MHz; Rx = 821 – 849 MHz) with a radio channel spacing of 30KHz and was first developed for use in North America; it was later deployed in Asia, Russia, and South America. TACS technology was first implemented in England and operated in both the 800MHz and 900MHz frequency bands (Tx = 935 – 960 MHz; Rx = 890 – 915 MHz) with a radio channel spacing of 25KHz; it was later deployed in Europe, Singapore, Hong Kong, and the Middle East. AMPS and TACS systems encode information with frequency modulation and have a spectrum allocation of 50MHz.

1.1.1 1G System Architecture

1G system uses full-duplex (two-way) communication as its means of radio transmission between the base station and mobile devices. This involves using separate transmit and receive frequencies whereby the cell unit transmits at the receive frequency of the mobile equipment. In contrast, the mobile device transmits at the receive frequency of the base station. 1G architecture typically consists of the mobile device, base station, Mobile telephone system office MTSO, and Public service telephone network (PSTN) as shown in figure 1.1.

- **Mobile phones**: These devices communicate via radio signal transmission with cell sites. Its primary purpose in the first generation technology is for voice communication.

Fig 1.1 1G System Architecture



Adapted from: Clint, S., Daniel, C. *3G Wireless Networks* (McGraw-Hill, 2002). https://www-accessengineeringlibrary-com.login.ezproxy.library.ualberta.ca/content/book/9780071363815

- **Base stations:** These cell sites send and receive information from mobile phones and mobile telephone system office MTSO. It communicates with mobile devices via radio transmission and uses either a microwave system or a T1/E1 leased line to connect to the MTSO. A base station consists of a monopole/tower, RF antennas, microwave/leased line, equipment room (which houses the base station controller, radio, amplifier, rectifier, battery, etc.), cable tray (which houses the coaxial cables connecting the radio equipment to the antennas).
- **Mobile Telephone System Office:** MTSO connects base stations via several cellular switches to the public switch (PSTN) and is responsible for call processing. It also maintains mobile subscribers' records, status, and billing information.
- **Public Service Telephone Network:** This public switching system relays a call (voice communication) from one network to another. It is an aggregation of circuit-switched telephone networks operated by local, regional, or national telephony operators to provide public telecommunication services.

1.1.2 Benefits of 1G Technology

- **Frequency reuse:** This is the process of reassigning the same radio frequency as many times as possible within a network geographical area. This network algorithm allows a cellular base station to have a higher capacity, allowing more users per geographical area.
- **Mobility of the subscribers:** This allows stationary devices, pedestrians with mobile phones, and moving vehicles to access the radio signal from a serving cell base station, irrespective of location, provided the serving cell has a good signal quality.
- **Handoff:** This is the process of transferring a call in progress from one cellular voice channel to another without interrupting the call. It can occur between sectors of the same or adjacent base stations, enabling the base stations to provide high capacity and operate at lower power levels. Handoff ensures that mobile equipment is connected to the best serving cell (for a quality call) as it transverses from one cell site to another.

1.1.3 Limitations of 1G Technology

- Limited system capacity due to the rapid growth in the popularity of mobile communication.
- Limited roaming between networks of different vendors due to unspecified network interfaces, as only the air interface was defined in its configuration.
- No security due to its analog-based means of communication, which led to theft and fraud.

1.2 2G Cellular Technology

Second Generation (2G) cellular network was the first digital mobile communication to utilize digital signaling for radio signals communication between a base station and end users. It was commercially launched as a Global System for Mobile Communication (GSM) standard in Finland in 1991and operates in the 900MHz frequency band (Tx = 925 – 960

MHz; Rx = 880 – 915 MHz) with a radio channel spacing of 200KHz. It was also deployed in the Digital Cross-connect System (DCS) 1800MHz band (Tx = 1805 – 1880 MHz; Rx = 1710 – 1785 MHz) and Personal Communications Services (PCS) 1900MHz (in North America) band (Tx = 1930 – 1990 MHz; Rx = 1850 – 1910 MHz). It uses the Regular Excited Linear Prediction Long Term Prediction (RELP-LTP) for digital speech coding, Gaussian Minimum Shift Keying (GMSK) modulations, and has a spectrum allocation of 50MHz. It offers advanced features such as increased security, improved speech quality, and international roaming.

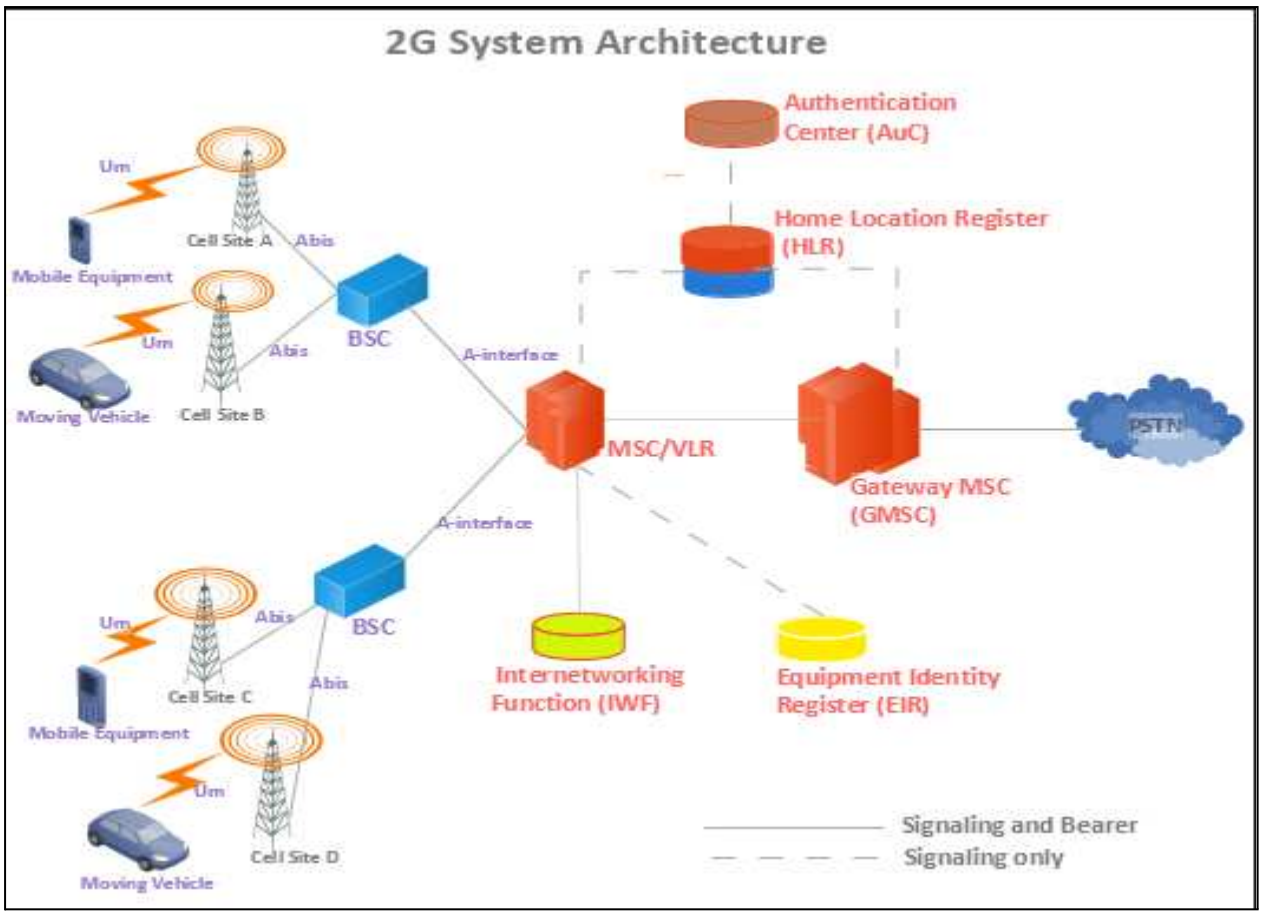
The two-channel access method employed by 2G technology was the Time Division Multiple Access (TDMA) which allows multiple end users to share the same frequency channel using different time slots (used in many countries across Africa, South America, Europe, and Asia) and also, Code Division Multiple Access (CDMA) referred to as cdmaOne or Interim standard IS-95 which employs spread spectrum technology allowing several mobile devices to send information simultaneously over a single communication channel using a unique coding scheme (widely employed in North America). It was initially developed as a circuit-switched network before the evolution of 2.5G and 2.75G, which implemented the packet-switched domain.

1.2.1 2G System Architecture

2G system, including its network architecture, interfaces, and services, were designed differently and incompatible with existing analog 1G technology. It also uses full-duplex (two-way) communication as its means of radio transmission between the base station and mobile devices. 2G network architecture as shown in figure 1.2 comprises the Mobile Station MS, radio access network, and the core network.

- **Mobile Station (MS):** This consists of both the Mobile Equipment (ME) and Subscriber Identity Module (SIM) card. The SIM card contains a tiny integrated circuit for storing user information, such as the subscriber's identity, authentication, and service information.

Fig 1.2 2G System Architecture



Adapted from: Clint, S., Daniel, C. *3G Wireless Networks* (McGraw-Hill, 2002). https://www-accessengineeringlibrary-com.login.ezproxy.library.ualberta.ca/content/book/9780071363815

- **Radio Access Network (RAN):** This consists of the Base Transceiver Station (BTS) and the Base Station Controller (BSC).
    - **Base Transceiver Station (BTS):** The BTS transmits and receives information from the mobile station via an Um air interface (radio signal path from the RF antennas) and usually a microwave link that connects to a hub site or directly to the Base Station Controller (BSC). A BTS consists of a cell tower, RF antennas, Outdoor Unit (ODU), a microwave link, an equipment room that houses the BTS boards, Indoor Unit (IDU) radio, rectifiers, batteries, etc., and a cable tray that houses the coaxial cables connecting the radio equipment to the antennas, and IF cable connecting the IDU radio to the ODU microwave.
    - **Base Station Controller (BSC):** A BSC interconnects one or more BTSs in a star topology via Abis interfaces, an Operation and Maintenance Link (OML) responsible for the configuration, operation, and maintenance of BTSs. It

provides unique functions such as subscribers' mobility management, radio resources management, and the network's operation, Administration, and Maintenance (OAM) management. It also connects to the Transcoding and Rate Adaptation Unit (TRAU), which converts coded speech to and from the standard 64kbps. BSC is called the Base Station Subsystem (BSS) in conjunction with BTS. In 2G technology, the Abis interface connection between a BSC and BTS is vendor compliant; this implies that the BSC can only be connected to a BTS from the same vendor. Furthermore, BSCs are independent of each other and have no connection to each other.

- **Core Network:** The primary core network nodes in a GSM network are the Mobile Switching Center (MSC), Home Location Register (HLR), Authentication Center (AuC), Equipment Identity Register (EIR), Internetworking Function (IWF), Gateway Mobile Switching Center (GMSC).
    - **Mobile Switching Center (MSC):** MSC is responsible for call setup, call routing, and various mobility management functions. It contains the Visitor Location Register (VLR), which stores each subscriber's information for the user's duration in the MSC coverage area. MSC connects to a BSC via A-interface, an SS7-based interface using its Signaling Connection Control Part (SCCP).
    - **Home Location Register (HLR):** This stores the database of all the subscribers on the network, including the services each user is provided.
    - **Authentication Center (AuC):** This is responsible for performing authentication algorithms between the AuC and SIM card.
    - **Equipment Identity Register (EIR):** It stores the 15 digits International Equipment Identity Number (IMEI) and also the Interworking Function (IWF) for circuit switched data and fax services.
    - **Interworking Function (IWF):** This node act as a dial-up modem and fax machine used to circuit-switched data and fax services. GSM supports these services up to a data rate of 9.6kbps.
    - **Gateway Mobile Switching Center (GMSC):** connects one or more MSCs to the Public Service Telephone Network PSTN. It is responsible for querying the Home Location Register (HLR) to determine a subscriber’s location when a call arrives from another network via a Public Service Telephone Network (PSTN). The call is then to the appropriate MSC serving the subscriber.

- **Public Service Telephone Network (PSTN):** This public switching system relays voice information in the standard 64Kbps Pulse Code Modulation (PCM) format from one network to another. It is an aggregation of circuit-switched telephone networks operated by local, regional, or national telephony operators to provide public telecommunication services.

1.2.2 Evolution of 2G Technology

1.2.2.1 2.5G Technology

The first technology advancement of 2G technology was the General Packet Radio Service (GPRS), known as 2.5G. It was established by European Telecommunication Standards Institute (ETSI) as a best-effort packet switch protocol for cellular network communication. Theoretically, it provides data rates of 56-114kbit/s. Still, it offers a maximum transfer speed of 40kbit/s, which only provides a little faster service due to the bundled timeslots in its circuit-switched domain. It solely depends on the number of users sharing the service concurrently.

1.2.2.2 2.75G Technology

The 2.75G technology, also known as Enhanced Data Rates for GSM Evolution (EDGE), was an advancement of the 2.5G that allowed an improved data transfer speed of 384kbit/s. It uses the 8PSK encoding allowing each symbol (3 bits per symbol) to be sampled at 270.833 samples per second. It is backward compatible with GPRS and requires no hardware or software changes in the GSM core networks. However, EDGE transceiver units must be installed at the base station, and the base station controller BSC needs to be upgraded for mobile users' access. AT&T first deployed EDGE in the United States in 2003.

1.2.3 Benefits of 2G Technology

- Information transfers between mobile devices and cellular base stations were digitally encrypted, increasing voice and data security.
- It enabled more end users to share a frequency band resulting in more efficient use of the radio frequency spectrum and increased capacity over 1G analog systems.

- It allowed for improved features, for example, data services such as short messaging service (SMS) and multimedia messaging service (MMS).
- Reduced capital infrastructure cost and overall capital per subscriber cost.

1.2.4 Limitations of 2G Technology

- Low data transfer speed for stationary devices, pedestrians, and moving vehicles.
- It could not handle complex data transfers such as audio and video streaming and fast internet access.
- Ease of security attacks: Poor encryption scheme (A5/1 stream cipher) used on the GSM network makes it susceptible to attack and exposes users of mobile devices to fraud and theft.

1.3 3G Cellular Technology

Third Generation (3G) network technology was an upgrade over the second Generation (2G) and its evolutions (2.5G GPRS and 2.75G EDGE) with faster data speed and more efficient voice quality. It was designed based on the International Mobile Telecommunication-2000 (IMT-2000) set of standards and specifications by the International Telecommunication Union (ITU). 3G initially provided an average data transfer rate of 2Mbps for stationary users, 384 Kbps for pedestrians, and 144 Kbps for moving vehicles; this resulted in rapid

market penetration for fixed wireless internet access, mobile Internet access, and mobile TV. However, Universal Mobile Telecommunication System (UMTS) was created and standardized by the 3rd Generation Partnership Project (3GPP) in 2001 and widely deployed in Canada, the USA, Europe, Africa, and part of Asia, while the CDMA2000 system was standardized by 3GPP2 in 2002 and used in South Korea, Southeast Asia, and China telecoms market.

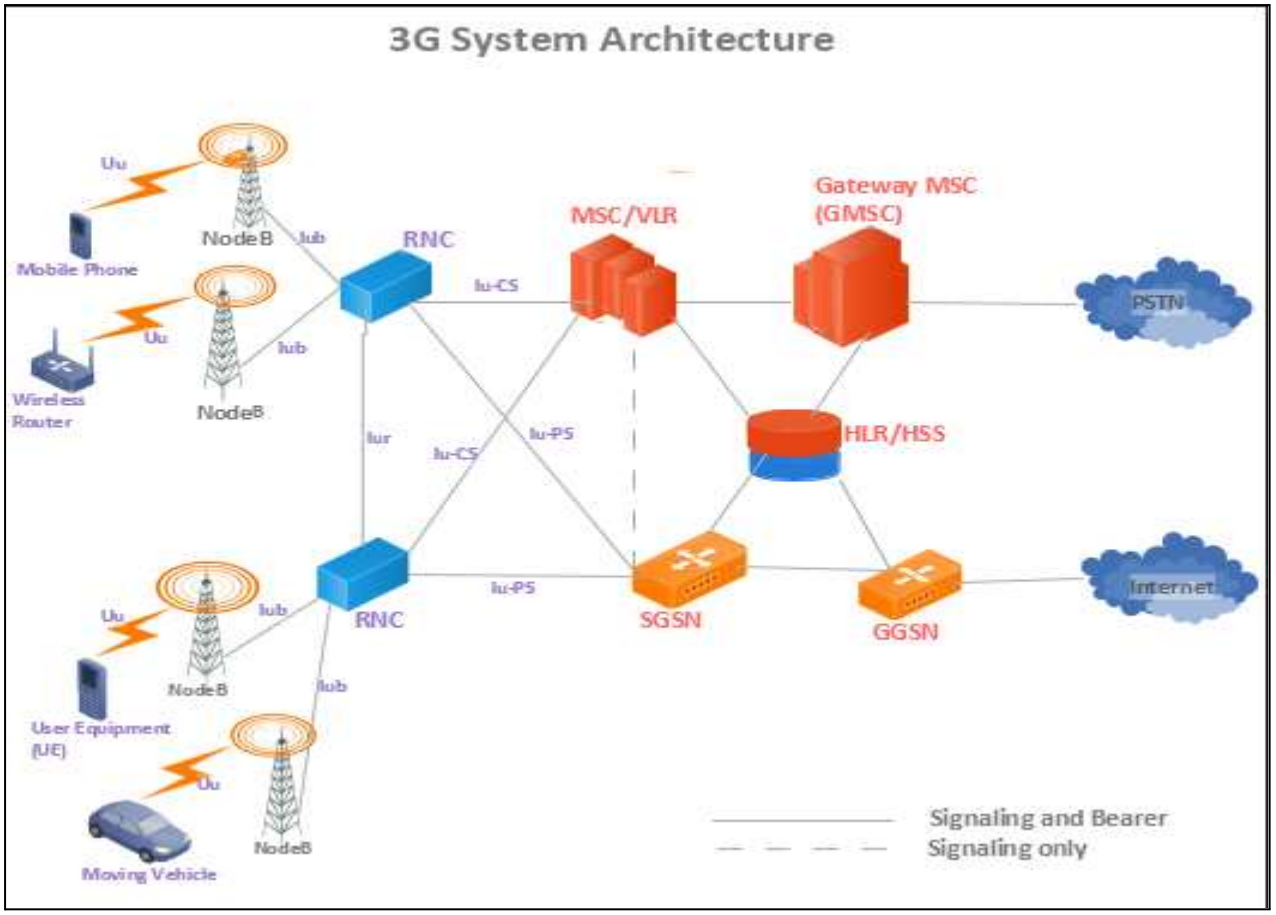
UTMS was an evolution of GSM, which supported 3G capabilities. It uses the Direct Sequence Wideband CDMA (DS-WCDMA) for both Frequency Division Duplex (FDD) and Time Division Duplex (TDD). The FDD, widely adopted globally, operates in the 1900MHz (1920MHz-1980MHz) band in the uplink and 2100MHz (2110MHz-2170MHz) band in the downlink with a separation of 190MHz between the uplink and downlink and a carrier spacing of between 4.4MHz to 5MHz. The TDD, common in the Asia telecom market, operates in the 1900MHz (1900MHz-1920MHz) band in the uplink and 2000MHz (2010MHz-2025MHz) band in the downlink and allows for a carrier to be used in both uplink and downlink.

1.3.1 3G System Architecture

The 3G system, including its network architecture, interfaces, and services, was designed to be backward compatible with existing GSM technology. It also utilizes full-duplex (two-way) communication as its means of radio transmission between the base station and mobile devices called the User Equipment. 3G network architecture as shown in figure 1.3 consists of the User Equipment (UE), Universal Terrestrial Radio Access Network (UTRAN), and the Core Network.

- **User Equipment (UE):** This contains the Mobile Equipment (ME) and the UMTS Subscriber Identity Module (USIM) card. The USIM card is a tiny chip that stores subscriber information, such as the subscriber's identity, security keys, and service information.

Fig 1.3 3G System Architecture



Adapted from: Clint, S., Daniel, C. *3G Wireless Networks* (McGraw-Hill, 2002). https://www-accessengineeringlibrary-com.login.ezproxy.library.ualberta.ca/content/book/9780071363815

- **Universal Terrestrial Radio Access Network (UTRAN):** combines the NodeB and Radio Network Controller (RNC).
    - **NodeB:** The NodeB transmits and receives information from the user equipment via a Uu interface (WCDMA air interface) and usually a microwave/fiber link that connects to a hub site or directly to an RNC. A NodeB station consists of a cell tower, RF antennas, Outdoor Unit ODU, a microwave link, an equipment room that houses the NodeB boards, Indoor Unit IDU radio, rectifiers, batteries, etc., a cable tray that houses the coaxial cables connecting the radio equipment to the antennas, and IF cable connecting the IDU radio to the ODU microwave.
    - **Radio Network Controller (RNC):** An RNC interconnects one or more NodeBs in a star topology via Iub interfaces (responsible for the logical operation maintenance of the NodeB). It controls the radio resources of all connected NodeBs and controls the subscribers' voice and packet data transfer

accessing the radio bearers. NodeB, in conjunction with RNC, is called Network Subsystem RNS. In 3G technology, the lub interface connection between a NodeB and RNC is fully standardized (not vendor compliant); this implies that the RNC can only be connected to a NodeB from a different vendor. Furthermore, RNCs are dependent on each other and are connected via the lur interface. This aids inter-RNC mobility and soft handover when a user moves between two NodeBs of different RNCs.

- **Core Network:** This primarily consists of the Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN) but also contains the MSC/VLR and Home Location Register (HLR) for GSM circuit-switched functions, therefore, creating room for 2G backward compatibilities and hand handover from 3G to 2G and vice-versa. It connects to the UTRAN via the lu interface and uses the Asynchronous Transfer Mode (ATM) technology in order to circuit-switched and packet-switched services.
    - **Serving GPRS Support Node (SGSN):** The SGSN provides packet-switched service for user equipment within its geographical service. It connects to the RNC in the UTRAN via the lu-PS interface. It also provides logical link and mobility management, packet routing, authentication, and billing functions. It contains the Visitor Location Register (VLR), which stores the database of information of each subscriber for the duration of the user in the SGSN coverage area.
    - **Gateway GPRS Support Node (GGSN):** It converts and forwards incoming data traffic from the user equipment via the SGSN to an external packet-switched network (such as the Internet) and vice versa. The GGSN connects one or more SGSNs to the Internet. It is also responsible for address mapping and assignment, IP pool management, and subscriber screening (being the default router for user equipment). GGSN, in conjunction with SGSN, is called the Support Nodes (GSN).

1.3.2 Evolution of 3G Technology

1.3.2.1 3.5G Technology

The first technology advancement of 3G technology was High-Speed Packet Access (HSPA), as known as 3.5G. HSPA is a combination of two cellular protocols, High-Speed Downlink Packet Access (HSDPA) and High-Speed Uplink Packet Access (HSUPA). It was introduced in 3GPP Release 5 and 6 as an improvement over the existing 3G technology to allow networks based on UTMS to have a higher data peak rate of up to 14Mbps in the downlink and 5.76Mbps in the uplink and also reduced latency and round-trip time in the cellular network communication. Advanced features in 3.5G, such as multi-code and shared-channel transmission, higher-order modulation, and fast hybrid automatic request (HARQ), resulted in enhanced data throughput. This allows for more applications such as VoIP and the upload of high-resolution images and bulk e-mails.

1.3.2.2 3.75G Technology

The 3.75G technology, also known as Evolved High-Speed Packet Access (HSPA+), was an advancement of the 3.5G and the technical standard for wireless broadband telecommunication. It was introduced in 3GPP Release 7 and provided a data transfer rate of up to 42Mbps by using advanced antenna technologies such as Multiple-Input, Multiple-Output (MIMO), and beamforming. Theoretically, other advanced HSPA+ technologies, such as 3GPP release 8 and 9, provide a peak data transfer rate of 84Mbps and 168Mbps in the downlink, respectively, while 3GPP release 11 allows for a peak data rate of up to 337Mbps under an ideal condition by using 64QAM modulation and Dual-Carrier HSDPA to the existing technologies.

1.3.3 Benefits of 3G Technology

- It allows for high broadband data throughput, capacity, and bandwidth required for fast internet access such as audio and video streaming, Global Positioning System GPS services, Voice over IP VoIP, etc.
- It provides higher voice quality and enables data-intensive applications to be developed and used.
- It provides a wider radio spectrum that allows for more users per cell within a geographical area.
- It allows for content-based and multimedia services such as mobile TV, video on demand, telemedicine, and global roaming.

1.3.4 Limitations of 3G Technology

- It results in complexity at both the UTRAN and core network design. Additional 3G compatible nodes, such as NodeB, SGSN, GGSN, etc., must be installed, configured, and connected to existing GSM nodes for circuit-switched services and hard handovers.
- High cost of purchasing a 3G spectrum license and agreement, and also high network deployment cost due to more cellular infrastructures installations, configuration, upgrades, and maintenance.
- High battery consumption of user equipment due to its on-mode internet access, and also, additional cost for end users to purchase 3G-enabled devices and pay for more data services.
- It is unsuitable for high data-intensive applications such high definition HD video streaming, interactive gaming, artificial intelligence, etc.

1.4 4G Cellular Technology

Fourth Generation (4G) network technology was the first cellular technology to incorporate an all-IP network architecture in its design. It was also referred to and marketed as Long Term Evolution (LTE) because it met the series of standards and policies set by the 3rd Generation Partnership Project (3GPP) for LTE. 4G technology adopted a flat architectural model with minimal nodes and a separate user and control plane function to solve network issues like cell breathing, low data throughout as users increase, low coverage area, and high

latency experienced in 3G networks. It enabled network operators to provide high-speed broadband service at a much-reduced latency rate and accommodate more users per cell. 4G spectrum bandwidth is categorized into the FDD band (1-25) and TDD band (33-43). Its bandwidth flexibility enables manufacturers of user equipment (UE) to add compatible chip sets to their devices based on the market's location.

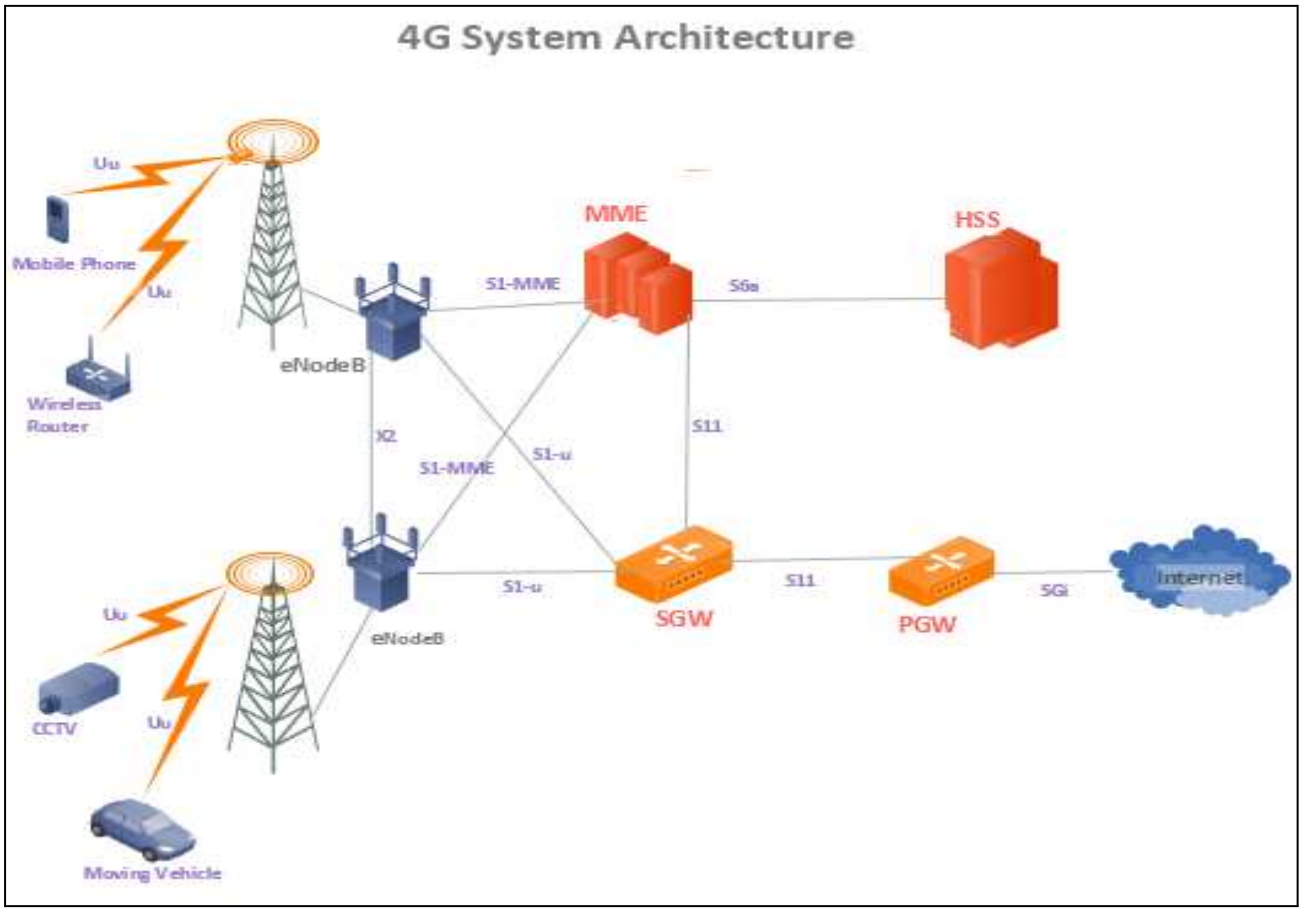
LTE specifications outlined in the 3GPP releases 8 and 9 have a maximum downlink speed of 100Mbps, maximum uplink speed of 50Mbps, latency round trip of approximately 10ms (resulting in its high-broadband speed), Frequency Division Duplex (FDD) spectrum of 10MHz. The channel access methods employed by LTE are Orthogonal Frequency Division Multiple Access (OFDMA) in a downlink and Single-Carrier Frequency Division Multiple Access (SC-FDMA) in an uplink. These FDMAs are an improved version of Frequency Division Multiplexing (FDM) technology and operate by dividing packets of information into separate bands and are carried by different signals.

1.4.1 4G System Architecture

4G adopts a flat architecture with an all-IP network in its design to meet its low latency demands. Low latency as a vital Quality of Service (QoS) parameter in a high-speed broadband network enabled it to be suitable for interactive games and high-definition HD video applications. 4G architecture as shown in figure 1.4 is simplified into three; User equipment (UE), Evolved-UMTS Terrestrial Radio Access Network (E-UTRAN), and Evolved Packet Core Network (EPC).

- **User Equipment (UE):** These are mobile (smartphones) devices and stationary (integrated into appliances, clothing, CCTV, vehicles, etc.) devices that communicate with the LTE wireless networks. Uu is the air interface for transporting signaling information and traffic data between the user equipment and the eNodeB.
- **E-UTRAN:** Enhanced NodeB (eNodeB) lies in the E-UTRAN network and serves as the middleman between the core network and UE for the LTE network connection. It consists of the radio unit, antennas, and digital processing unit. The eNodeB dynamically allocates network resources to the User Equipment in both the downlink and uplink using a scheduler process. It also carries out radio resource management (RRM) functions such as Radio Mobility Control (RMC) and Radio Bearer Control (RBC).

Fig 1.4 4G System Architecture



Adapted from: Juha, K. (2014). *Introduction to 4G Mobile Communications*. Artech House.

eNodeB utilizes the OFDMA and SC-FDMA modulation schemes for its downlink and uplink RF channel, respectively. Two eNodeBs in the E-UTRAN network can be connected via an X2 interface for coordinating handover and data transfers. Furthermore, eNodeB routes data traffic to the EPC via the Serving Gateway (SGW) connected via Signaling S1-U and controls information to the EPC via the Mobility Management Element (MME) connected via signaling S1-MME.

- **Evolved Packet Core (EPC):** The EPC houses the core network devices and uses IP as the main protocol in its packet-switched domain. The circuit-switched domain was primarily not integrated into the LTE architectural design to achieve low latency. The primary core network nodes in a 3GPP RAN Serving Gateway (SGW), Mobility Management Entity (MME), Packet Data Network Gateway (PGW), and Home Subscriber Server (HSS).
    - **Serving Gateway (SGW):** It routes data traffic from the UE to the core network and acts as the mobility anchor as UE moves from one eNodeB to another, thereby allowing the UE to be connected to the same SGW. It also

manages handover between eNBs, network regulation compliances, network service requests, and deliveries. It is connected to the MME via the signaling S11 link and interconnects with other 3GPP technologies, such as UTMS.

- **Mobility Management Entity (MME):** It routes control information from the UE to the EPC and also determines the Packet Gateway (PGW) and Serving Gateway (SGW) the UE will connect to based on the information gathered from the Home Subscriber Server HSS. It makes the UE be in the connected/registered state, Idle/Inactive state, or dormant/Not connected state. It also manages UE authentication, billing, and load balancing. MME interface with the SWG via the signaling S11 link and the HSS via the signaling S6a link.
- **Packet Data Network Gateway (PGW):** It allocates an IP address to the user equipment (UE) and filters downlink IP packets based on enforced Quality of Service (QoS) rules from the Policy Control and Charging Rule Function (PCRF). It is connected to the SGW via the signaling S11 link and interconnects with non-3GPP technologies like CDMA2000.
- **Home Subscriber Server (HSS):** This contains the database of users' subscription information in the LTE network. This includes users' current location data, authentication keys, roaming and quality of service profile, etc.

1.4.2 Evolution of 4G Technology

1.4.2.1 LTE-Advanced

The LTE-A introduced new features and functionalities like intra and inter-frequency carrier aggregation, relay nodes, coordinated multipoint, enhanced multi-antenna techniques (diversity MIMO, up to 8x8 MIMO on the downlink, and 4x4 MIMO on the uplink), higher spectral efficiency up to 30bps/Hz in downlink and 15bps/Hz in the uplink, increased number of active users per cell (data modulations support QPSK, 16QAM and up to 256QAM modulation for both downlink and uplink). These key improvements led to an increase in both downlink and uplink data throughput. It also has an enhanced precoding mechanism, forward error correction capabilities, and improved interference management using Inter-cell Interference Coordination (ICIC). It supports autonomous network configuration with Self-organizing networks (SON) enhancement.

LTE-A specifications outlined in the 3GPP release 10 have an initial maximum downlink speed of 1Gbps, maximum uplink speed of 500Mbps (this was later increased to 3Gbps DL and 1.5Gbps UL), latency round trip of approximately 10ms, Frequency Division Duplex (FDD) multicarrier with a bandwidth of up to 100MHz of the spectrum Although, both FDD and TDD are supported, FDD is widely used. The channel access methods employed by LTE-A are Orthogonal Frequency Division Multiple Access (OFDMA) in the downlink and a hybrid of OFDMA and Single-Carrier Frequency Division Multiple Access (SC-FDMA) (Discrete Fourier Transform DFT spread OFDM) in the uplink. These FDMAs are an improved version of Frequency Division Multiplexing (FDM) technology and operate by dividing packets of information into separate bands and are carried by respective signals.

1.4.3 Benefits of 4G Technology

- It allows for high broadband data throughput, capacity, and bandwidth required for high-definition HD video streaming, interactive gaming, artificial intelligence, etc.
- It provides better spectral efficiency due to its broad range of frequency bands.
- It supports multimedia services at a lower transmission cost.
- Increased level of synchronization and data security.

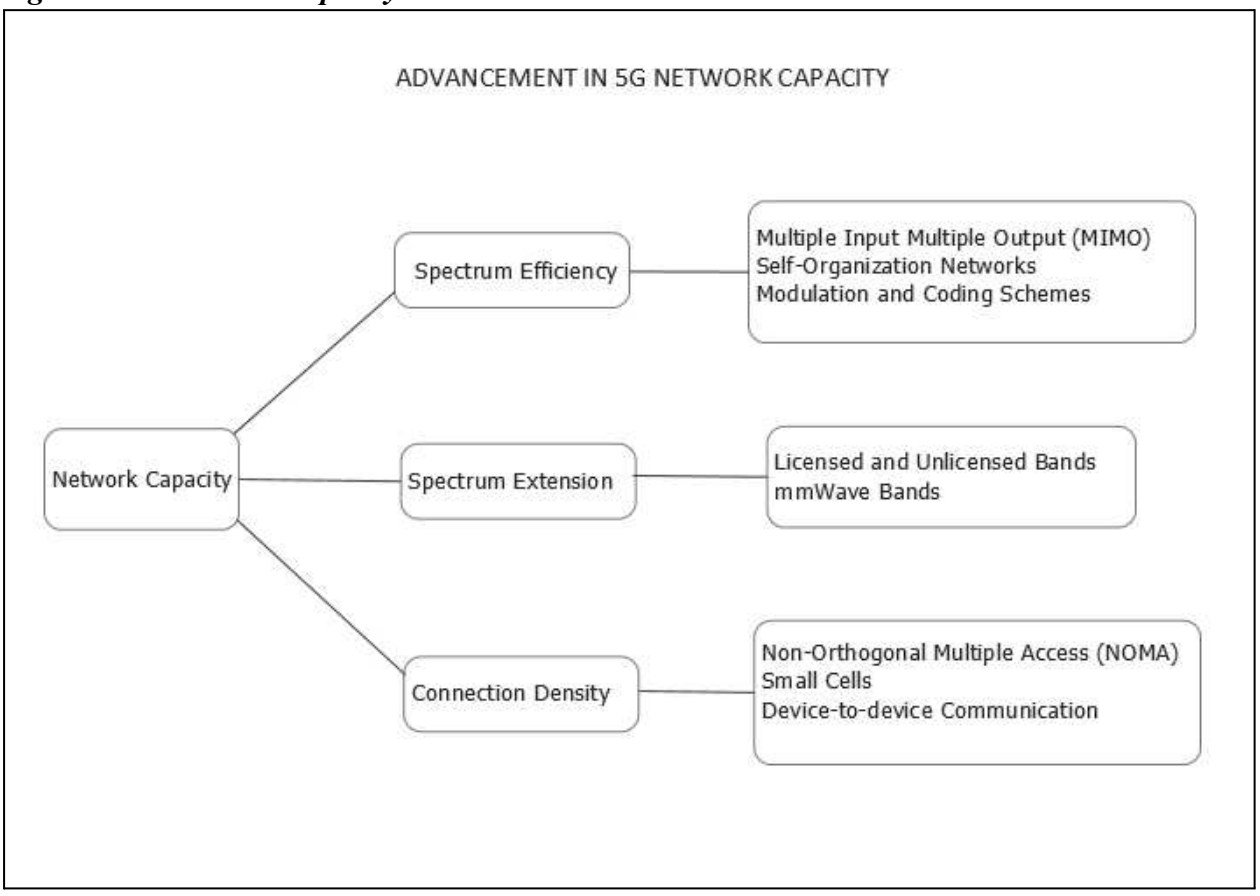
1.4.4 Limitations of 4G Technology

- High cost: This applies to both end users and network operators. End users are required to purchase new user equipment that is compatible with the available frequency spectrum. On the other hand, network operators need to deploy and install new nodes at both the radio access and core network, which are not backward compatible with previous technologies.
- Great reduction in the battery life of user equipment due to multiple antennas (transmitters and receivers) used by 4G mobile networks.
- It is not optimal for highly intensive data applications such as mobile edge computing, autonomous vehicles, machine-to-machine communication, and the massive Internet of Things.

Chapter 2: 5G Network Technology

5G network technology is fast evolving in the 21st century to keep up with the requirements for high-speed data rates. According to the GSM Association and Statista, it is predicted to provide network coverage to more than 1.7 billion subscribers and about 25% of the world mobile technology market by 2025. Higher network capacity, high user mobility, and enhanced connectivity have been some of the major determining factors in 5G network design compared to the previous LTE technology. Advanced technology, such as improved spectrum efficiency using MIMO and self-organization networks, spectrum extension by including unlicensed and mmWave bands, and increased connection density using small cells and NOMA, were introduced as proposed by the International Telecommunication Union (ITU-R) IMT-2020. The figure 2.1 below shows the trends in 5G network capacity:

Fig 2.1 5G Network Capacity



Adapted from: Ghonge, M., Mangrulkar, R. S., Jawandhiya, P. M., & Goje, N. (2021). *Future Trends in 5G and 6G : Challenges, Architecture, and Applications* (p. 129), 2022. CRC Press.

5G services support for multi-carrier systems, advanced data modulation, and coding schemes would positively impact its network capacity and interoperability among the

network operators, resulting in better revenue. It's smart beam antennas; that is, beamforming technology would help to reduce interference to the minimum. It would provide better security, a better quality of service, and lower battery consumption than previous technologies.

2.1 5G Service Requirements

The service requirements for 5G proposed by the International Telecommunication Union (ITU-R) IMT-2020 are as follows:

- **Peak data rate:** This is the maximum achievable data rate per user under an ideal condition and is measured in bits per second. The minimum requirements for enhanced Mobile Broadband (eMBB) peak data rate are 20Gbps in the downlink and 10Gbps in the uplink.
- **Peak spectral efficiency:** This is the maximum data rate under an ideal condition normalized by the channel bandwidth and measured in bits per second per hertz. 5G NR uses Multiple Input Multiple Output (MIMO) technologies to increase the capacity by implementing multiple transmissions and multiple receptions mechanism. The minimum requirements for eMBB peak spectral efficiencies are 30bps/Hz in the downlink and 15bps/Hz in the uplink.
- **User-experienced data rate:** This is the achievable data rate experienced by mobile users or devices within a coverage area. The targeted values for the user-experienced data rate in a densely urban eMBB test environment are 100Mbps in the downlink and 50Mbps in the uplink.
- **Reliability:** This can be defined as the ratio of a successfully transmitted data packet to the total transmitted data packet within a given time. The minimum requirement for reliability in a densely urban environment to transmit 32 bytes of MAC packets in less than 1 ms is 99.999%.
- **Bandwidth:** This is defined as the maximum aggregated system bandwidth. The minimum required bandwidth for 5G service is 100MHz. Although, ITU-R supports and encourages a bandwidth of more than 1GHz to be used by proponents.
- **User plane latency:** refers to a packet's transition time from a source to the destination. The minimum requirements for a one-way end-to-end latency over the radio interface are 4 ms for eMBB and 1 ms for Ultra-Reliable Low Latency Communications (URLLC).

- **Control plane latency:** This is defined as the transition time from an ideal or inactive state to an active state. The minimum requirement for control plane latency is 20ms, though; there are considerations for lowering the control plane latency to 10ms as proposed by the 3rd Generation Partnership Project 3GPP.
- **Connection density:** It is defined as the total number of network devices that can be connected per unit area. The minimum requirement for massive Machine Type Communication (mMTC) connection density is 1,000,000 devices per km^2.
- **Mobility interruption time:** This is defined as the time during which data packets cannot be exchanged between 5G devices as a result of handover (make before break) procedures. During this process, the control plane is connected to the lower frequency band while the data plane is connected to the cells often used capacity. The minimum requirement for both enhanced Mobile Broadband (eMBB) and Ultra-Reliable Low Latency Communications (URLLC) mobility interruption time is 0ms.
- **Energy efficiency:** The energy efficiency of the radio access network or gNB is defined as the number of packets transmitted to or received from users measured in bits per unit of energy consumption (bits/Joule) of the RAN. On the other hand, the energy efficiency of the user device is the number of information bits per unit of energy consumption (bits/Joule) of the network device. In both cases, air interfaces must support long sleep duration and high sleep ratio.

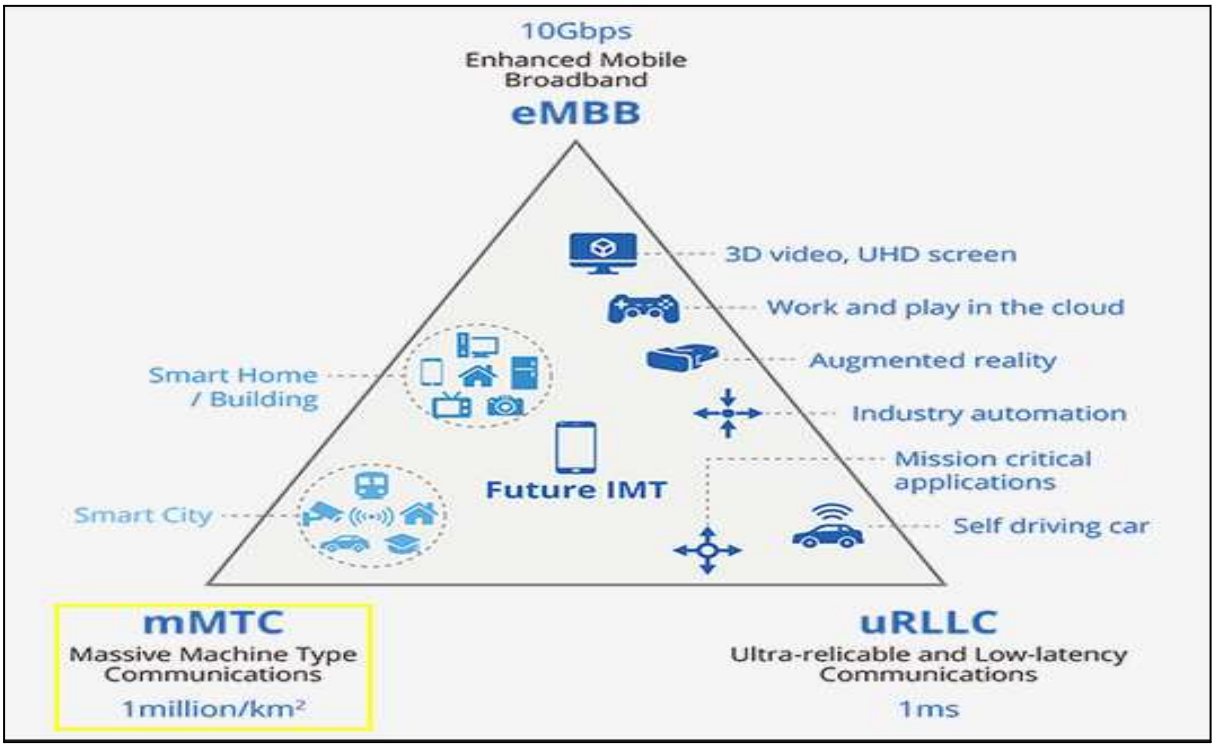
2.2 5G Service Types

The main service types for the 5G New Radio NR standard defined by the 3rd Generation Partnership Project 3GPP telecommunication standard group and illustrated in figure 2.2 are as follows:

2.2.1 Enhanced Mobile Broadband (eMBB)

This is an advancement over the 4G Long Term Evolution LTE, allowing for both improved performance and an increasingly seamless user experience. The 5G NR enables faster data transmission rate, more bandwidth capacity, and lower latency which offers fast fixed wireless access (FWA) to residential, business, and mobile users. This allows direct network connections to network devices beyond smartphones and Wi-Fi to other mobile devices such as connected vehicles (police cars, ambulances, safety vehicles, etc.), mobile routers, laptops, IP TV, security cameras, gaming consoles, etc., and also, enabling access to services such as automobile infotainment, mobile 4K video streaming, 3D multi-player video games, etc.

Fig 2.2 5G Service Types & Usage Scenario



From: *[5G-mmtc]smart city solution: Solution - gigabyte global*. GIGABYTE. (n.d.). Retrieved October 29, 2022, from https://www.gigabyte.com/Solutions/mmtc

Enhanced mobile broadband has three main attributes which are:

- **Higher capacity:** It will provide broadband access in densely populated outdoor and indoor areas with low user mobility, such as city centers, stadiums, theatres, cinemas, etc.
- **Higher user mobility:** It will provide comprehensive area coverage with medium to high user mobility areas such as trains, planes, and buses.
- **Enhanced connectivity:** It will allow for a seamless user experience anywhere and anytime.

2.2.2 Ultra-Reliable and Low-latency Communications (URLLC)

This is one of the mission-critical capabilities in a 5G network that would use a different Quality of Service (QoS) to provide an instantaneous and intelligent network system. According to the 5G New Radio (NR) standard stipulated by the 3rd Generation Partnership Project 3GPP Release 15 and 16, URLCC will be ideal for applications classified in table 2.1 that require 1ms data plane latency, 0ms mobility interruption time, 99.999% reliability, end-to-end security, and 100% availability for effective packet delivery. This will be

applicable in extremely low latency and susceptible connected devices in critical use cases as follows:

- **Autonomous Driving:** URLLC will enhance the use of driverless cars for both private and commercial purposes. This will require stringent requirements such as 1ms latency, 99.999% reliability, and support of high-speed mobility of up to 240km/hr. It will also provide enhanced driver assistant applications, vehicle platooning, high-definition maps, etc.
- **Emergency Response:** This would enhance first responders' services such as police, firefighter services, and hospital ambulances, thereby improving care administered in the case of robbery, fire incidents, and accidents, respectively. For example, real-time communication, such as live videos via multiple sensors, can be shared between field doctors in an ambulance with the back office to improve health services (diagnosis and remote surgeries) administered to accident victims.
- **Smart Grid:** 5G network would help improve the smart power grid system with a distributed feeder that requires less than 5ms latency and 99.999% reliability. It would enhance load balance and control during power grid failure, thereby preventing fatal damage to the grid system.
- **Smart Factory:** 5G networks would allow next-generation factories to create a prevalent network of automated machinery for production and other business activities. It would be applicable in processes such as machine-to-machine communication, real-time robotic control, motion control machines, video-machine interaction, etc.
- **Industrial Remote Guided Vehicles:** 5G would utilize its low latency; and high sensitivity network attributes to enable remote management of guided vehicles to be possible in a hazardous industrial environment such as sea ports, mines, construction industries, etc.

Table 2.1 URLCC case study

Industry	Application
Healthcare	Emergency Response Remote Diagnosis Remote Surgery

Transportation	Driverless Cars Driver Assistant Applications Intelligent Transport Traffic Management
Entertainment	Online Gaming Immersive Entertainment
Energy	Smart Grid Smart Energy
Smart Factory	Machine to Machine communication Process control Robotics and automation
Manufacturing	Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR) Applications Motion Control Remote Control

2.2.3 Massive Machine Type Communication (mMTC)

5G networks would enable the connection of a large number of residential and commercial devices for easy interaction and internet services, thereby resulting in a significant transformation in the Internet of Things (IoT) Industry. According to the 5G New Radio NR standard stipulated by the 3rd Generation Partnership Project 3GPP Release 15 and 16, the minimum requirement for massive Machine Type Communication (mMTC) connection density is 1,000,000 devices per $km^{2,}$ which meet the demands of smart cities. mMTC will drive the enormous production of low-power devices with embedded sensors at a low cost. It offers low bandwidth with in-depth coverage, which would enable IoT devices to transmit a small amount of non-delay sensitive data, which would contribute to its long battery life. This would be applicable for low bandwidth devices following use cases:

- **Residential:** mMTC would allow a large volume of sensors to utilize 5G networks for smart metering of household utilities such as gas, water, thermostat, and electricity.

- **Smart cities:** This would enable sensors to be placed around the city for data collection and analysis for the overall improvement of the resident's quality of life. This includes sensors-embedded radar counters, traffic cameras, and air quality counters for effective management of waste, traffic, parking, public vehicles, and the environment.
- **Logistics:** It would allow for easy management of tracking devices such as tagged objects used in the fleet and logistics industry for monitoring the exact location of an item.

2.3 Spectrum Sharing

5G wireless networks can utilize frequency bands to support data services required in smart homes, smart grids, smart cities, autonomous vehicles, blockchain, augmented reality, video surveillance systems, and high-speed internet. These bands are classified into three as follows:

- **Low Band:** This uses a frequency range less than 1GHz, usually between 600 - 850 MHz for 5G services, has more excellent coverage, and provides a speed of up to 250Mbps
- **Mid Band:** This corresponds to the frequency range of 1- 6GHz, but is allocated between 2.5 – 3.7 GHz for 5G services and provides a speed of up to 900Mbps
- **High Band:** Also known as millimeter wave (mmWave) band. This uses a frequency range of between 24 GHz and 40 GHz and provides a speed of up to 1Gbps but a smaller coverage area.

Spectrum sharing refers to the operation of two or more radio systems in the same frequency band. It maximizes the use of available frequency bands for mobile broadband systems to meet the increasing data traffic needs of end users. The two popular spectrum-sharing models in the 21st century are the European two-tier model of Licensed Shared Access (LSA) and the United States three-tier model of Citizen Broadband Radio Services (CBRS).

2.3.1 Licensed Shared Access (LSA)

This spectrum-sharing model was proposed by the European Commission (EC) to allow any radio system to share an existing frequency band. It is determined by the agreed sharing framework between stakeholders, and the LSA license is issued by the National Regulatory

Authority (NRA). The level of access rights in the European spectrum sharing is a two-tier model: Incumbent Access (IA) and LSA licensed. Incumbent spectrum users are given more privileges, and they decide the frequency bands to the shared in different geographical locations.

2.3.2 Citizen Broadband Radio Services (CBRS)

This is a three-tier sharing model adopted by the Federal Communications Commission (FCC) in April 2015. It was first proposed by PCAST (President's Council of Advisors on Science and Technology) in 2012. CBRS utilizes the 3.5GHz (3550-3700MHz) band and adopts a three-tier model, which are Incumbent Access (IA), Priority Access (PA), and General Authorized Access (GAA) to accommodate small cells, point-to-point and point-to-multipoint for rural coverage. The Spectrum Access System (SAS) coordinates the spectrum usage of entrants and manages interference for incumbent users' protection. Incumbent Access IA users have primary spectrum rights anywhere and anytime over Priority Access (PA) and General Authorized Access (GAA). All Citizen Broadband Radio Service Devices (CBSDs) and End User Devices (EUDs) can establish two-way communication across the entire 3.5GHz band. The 3550-3650MHz spectrum is allocated for use by the US Department of Defense (DoD) radar systems and Fixed Satellite Services (FSS), while the 3650-3700MHz spectrum is allocated to the FSS and Wireless Broadband Services.

2.4 5G Air Interface

At the physical layer of 5G network connections, downlink (DL) and uplink (UL) physical channels are defined. This includes the frame structure, physical resources, modulation mapping, coding scheme, etc. The physical channel provides an interface between the user equipment UE and Radio Access Network or gNodeB and also carries both the user and control plane data. 5G NR uses the following physical layer features at both the downlink (DL) and uplink (UL) direction for communication:

- **Duplex:** 5G NR uses both the Frequency Division Duplex (FDD) and Time Division Duplex (TDD) for transmission in both the unpaired and paired spectrum.
- **Multiple Access Scheme:** The physical layer uses Orthogonal Frequency Division Multiplexing (OFDM) with a cyclic prefix (CP) in the downlink (DL) and Discrete Fourier Transform-spread-OFDM (DFT-s-OFDM) with a cyclic prefix (CP) in the uplink (UL).

- **Modulation and coding scheme:** The physical layer of 5G NR supports QPSK, 16QAM, 64QAM, and 256QAM for CP-OFDM in the downlink (DL); and also pi/2-BPSK, QPSK, 16QAM, 64QAM, and 256QAM for DFT-s-OFDM in the uplink (UL).
- **Channels:** 5G NR has the Physical Data Shared Channel (PDSCH) for carrying user data, the Physical Downlink Control Channel (PDCCH) for carrying Downlink Control Information (DCI), and Physical Broadcast Channel (PBCH) for broadcasting Master Information Block (MIB) in the downlink (DL); and also the Physical Random Access Channel (PRACH) for user access request, Physical Uplink Shared Channel (PUSCH) for carrying user data and Physical Uplink Control Channel (PUCCH) for conveying Uplink Control Information (UCI) in the uplink (UL).

Table 2.2 Difference between LTE and 5G Air Interface

Parameters	LTE	5G
Channel Coding	Turbo coding (data) Convolution coding (control)	LDPC (data) Polar codes (control)
Frame	15 kHz	Flexible (15kHz, 30kHz, 60kHz, 120kHz)
Initial Access	No beamforming	Beamforming
Latency (Air interface)	10ms	1ms
Duplexing	FDD, Static TDD	Flexible TDD
Modulation Scheme	Pi/2 BPSK on the uplink is not supported	Pi/2 BPSK on the uplink is supported
Waveform	CP-OFDM for DL SC-FDMA for UL	CP-OFDM for DL DFT-s-OFDM for UL
Maximum Bandwidth	20MHz	50MHz (@15kHz) 100MHz (@30kHz) 200MHz (@60kHz) 400MHz (@120kHz)

Adapted from: Ghonge, M., Mangrulkar, R. S., Jawandhiya, P. M., & Goje, N. (2021). *Future Trends in 5G and 6G : Challenges, Architecture, and Applications* (p. 129), 2022. CRC Press.

2.5 5G NETWORK ARCHITECTURE

Fig 2.3 5G Network Architecture

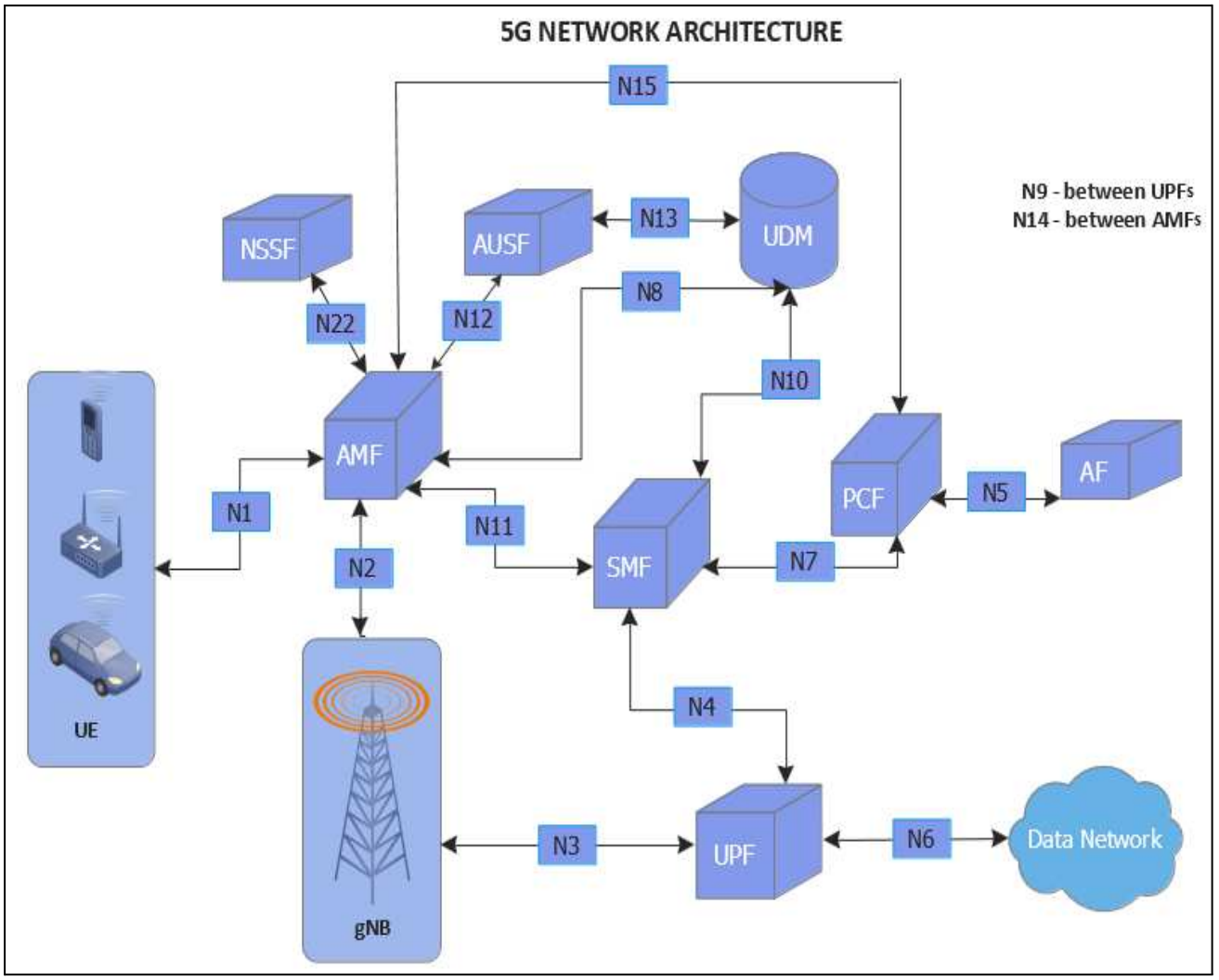


Table 2.3 Functional blocks within 5G Network architecture

Abbreviation	Functional Block
UE	User Equipment
RAN/gNB	Radio Access Network or gNodeB
AMF	Core Access and Mobility Management Function
SMF	Session Management Function
UPF	User Plane Function
PCF	Policy Control Function
AF	Application Function
DN	Data Network, e.g., operator services Internet or 3rd party services
UDM	Unified Data Management
AUSF	Authentication Server Function

NSSF	Network Slice Selection Function

Table 2.4 3GPP specification for 5G reference points

Reference Points	Function Description
N1	Between UE (User Equipment) and AMF (Core Access and Mobility Management Function)
N2	Between RAN (Radio Access Network) or gNB (5G Base Station) and AMF (Core Access and Mobility Management Function)
N3	Between RAN (Radio Access Network) or gNB (5G Base Station) and UPF (User Plane Function)
N4	Between SMF (Session Management Function) and UPF (User Plane Function)
N5	Between PCF (Policy Control Function) and AF (Application Function)
N6	Between UPF (User Plane Function) and DN (Data Network)
N7	Between SMF (Session Management Function) and PCF (Policy Control Function)
N8	Between UDM (Unified Data Management) and AMF (Core Access and Mobility Management Function)
N9	Between two core UPFs (User Plane Function)
N10	Between UDM (Unified Data Management) and SMF (Session Management Function)
N11	Between AMF (Core Access and Mobility Management Function) and SMF (Session Management Function)
N12	Between AMF (Core Access and Mobility Management Function) and AUSF (Authentication Server Function)
N13	Between UDM (Unified Data Management) and AUSF (Authentication Server Function)
N14	Between two AMFs (Core Access and Mobility Management Function)
N15	Between PCF (Policy Control Function) and AMF (Core Access and Mobility Management Function) in case of a non-roaming scenario, V-PCF, and AMF in case of a roaming scenario
N16	Between two SMFs (Session Management Function) in roaming case between V-SMF and the H-SMF

N22	Between AMF (Core Access and Mobility Management Function) and NSSF (Network Slice Selection Function)

2.6 5G Network Functions

2.6.1 Core Access and Mobility Management Function (AMF)

- Access point for UE and mobility management: AMF serves as the access point for UE to communicate with the 5G core network and also the mobility management of UE as it moves from one gNB to another.
- Subscriber location: AMF helps to track the subscriber's location via its cell ID when the UE is in the active state and via its tracking area ID if in the idle state. As a subscriber moves from one tracking area to another, AMF stores the specific UE list of tracking areas in a registration area. This eliminates signaling overhead caused by frequent mobility updates as a UE moves from one tracking area to another.
- It plays a key role in authenticating the subscriber by connecting to the Authentication Server Function (AUSF).
- It helps in cyphering/encrypting and data Integrity protection as packets move to and from the user equipment.
- It allocates a temporary ID called a Globally Unique Temporary ID (GUTI) to the user equipment (UE).

2.6.2 Session Management Function (SMF)

- Session management (SMF) enables the creation, modification, and termination of PDU sessions.
- Liaison with PCF for policy and QoS enforcement: It gets the PCC rule from the policy control function PCF and uses these rules to enforce quality of service unto the PDU sessions used by the UE.
- It allocates an IP address to the UE if the packet flow is IP traffic.
- It helps in the selection and control of UPF to the appropriate UE.
- It provides the Quality of Service (QoS) rule to the UE, QoS profile to the radio access network (gNodeB), and SDF template to the UPF.

2.6.3 User Plane Function (UPF)

- It acts as an anchor point during the NG RAN mobility.
- It ensures and maintains good quality of service QoS.
- It enables service data flow SDF filtering and applies QoS Flow ID.
- It allows for packet routing and forwarding.

2.6.4 Unified Data Management (UDM)

- It contains a central registry of subscriber information and a data network profile.
- It allows access authorization for subscribers by using encrypted keys. This streamlines the allowed AMF and SMF; and also the QoS profile or data network a UE can connect to, thereby enhancing security.
- It is involved in the registration and mobility management of UE.

2.6.5 Policy Control Function (PCF)

- It takes dynamic decisions based on the present network condition. For example, if a subscriber is in a poor or no coverage area, PCF can instruct SMF to reduce the data rate or not allow PDF sessions.
- It takes a proactive decision on the appropriate allocation of network resources.

2.7 Benefits of 5G Technology

- It allows the connection of heterogeneous networks seamlessly and is also backward compatible with 3G and 4G devices.
- It is capable of providing better Quality of Service (QoS) and new user services, such as cloud gaming, intelligent transport, process control, etc., at a very high data transfer speed.
- It is optimal for highly intensive data applications such as mobile edge computing, autonomous vehicles, machine-to-machine communication, and the massive Internet of Things.

Chapter 3: Private Wireless Networks

3.1 Private Network Spectrum

The rapid growth of wireless demand and internet connectivity in the 21st century has resulted in an equally proportional need for spectrum allocation to operate wireless devices. Unfortunately, most countries where wireless services exist have a limited spectrum. They are often left with the option of terminating or relocating existing spectrum services in a geographical location to be used in another. Each successive spectrum reallocation has been more costly regarding its termination at the existing domain and using the band in the new incumbent domain. These complexities result from extreme difficulty and cost-effectiveness in reclaiming the spectrum. For example, a licensed spectrum user carries out its radio and system designs, operating policy, and business planning based on its allocated spectrum band, thereby developing a strong resistance to any changes to the reallocation or termination of the existing spectrum. The spectrum scarcity has resulted in huge investments by the government, commercials, the military, etc. It has also led to wireless system limitations to meet increasing broadband demands.

One of the major setbacks of the traditional model of spectrum usage was the provision of an exclusive right of a portion of the spectrum to a single user in a specific geographical location. This approach had challenges and disadvantages, such as geographic exclusivity, usage exclusivity, and obsolete spectrum allocation. Firstly, geographic exclusivity, which is the allocation of spectrum to licensed or permitted users such as Mobile Network Operators (MNOs), across a large geographical region, resulted in the under-utilization of the spectrum at some sparsely populated locations and the starvation of spectrum at densely populated locations. Secondly, usage exclusivity, which is the allocation of spectrum to permitted users for a single purpose such as satellite television broadcast, land radio, and television services, etc., has resulted in the unavailability of the spectrum for other congruent services. Thirdly, some allocated spectra have become obsolete due to technological advancement. For example, most microwave links have been replaced with fiber optic links due to their high data bandwidth speed and non-susceptibility to electromagnetic interference; satellite television broadcasts are rapidly fading and replaced with high-definition streaming television services such as Netflix, Amazon prime video, Apple TV, etc. over the Internet.

Spectrum sharing is now being adopted and has become a possible solution to address the scarcity and setbacks of spectrum allocation. This technical innovation enables spectrum to be allocated to new services without terminating the existing ones. With the advent of 5G technology, which would involve the deployment of network infrastructure and small cells network devices on a building-by-building and room-by-room basis, spectrum sharing would allow both public network operators and non-traditional operators such as enterprises, industry, and government to have access to common spectrum and infrastructure technologies. It would increase the range of business organizations that can deploy wireless technologies and private networks at a reduced and shared cost, in addition to its advantage of providing higher bandwidth services.

3.2 Citizen Broadband Radio Services (CBRS)

Citizen Broadband Radio Services (CBRS) is a three-tier sharing model adopted by the Federal Communications Commission (FCC) in April 2015. It was the framework and approach proposed by the President Council of Advisors on Science and Technology (PCAST) in 2012 to address the challenges of spectrum scarcity. CBRS utilizes the 3.5GHz (3550-3700MHz) band, which is a licensed sharing layer and an opportunistic sharing layer with different levels of access rights. The 3550-3650MHz spectrum is allocated for use by the US Department of Defense (DoD) radar systems and Fixed Satellite Services (FSS), and the 3650-3700MHz spectrum is assigned to the FSS and Wireless Broadband Services.

It adopts a three-tier model, which are Incumbent Access (IA), Priority Access (PA), and General Authorized Access (GAA) to accommodate small cells, point-to-point, and point-to-multipoint for both densely populated and rural coverage. The main purpose of the Citizen Broadband Radio Service (CBRS), as stated in its final rule-making, is “to take advantage of advances in spectrum policy and technology to dissolve traditional regulatory spectrum divisions between commercial and federal users, public carrier and private networks, and also, exclusive and non-exclusive authorizations." The Spectrum Access System (SAS) coordinates the spectrum usage of entrants and manages interference for incumbent users' protection. All Citizen Broadband Radio Service Devices (CBSDs) and End User Devices (EUDs) can establish two-way communication across the entire 3.5GHz band.

3.2.1 CBRS Sharing Model

The CBRS sharing framework consists of Incumbent Access (IA), Priority Access (PA), and General Authorized Access (GAA). Based on FCC rules, the IA users have primary spectrum access rights at all times and in all locations over PA and GAA users and must be protected from harmful interference. All users in the sharing framework can operate across the entire 3.5 GHz band, terminate operation, and change frequencies in the Spectrum Access System (SAS) direction to protect Incumbent Access users. The SAS also carries out automated channel assignments with detailed information instructions for users to use a specific channel at a specific location and time within the 3,550 – 3,700 MHz frequency range.

3.2.1.1 Incumbent Access

Incumbent Access (IA) users have primary spectrum rights anywhere and anytime over Priority Access (PA); and General Authorized Access (GAA). This is utilized by the United States Navy and Fixed satellite services. Based on FCC rules, it is mandatory for all PA and GAA users to protect the IA users in the band.

3.2.1.2 Priority Access License

The Priority Access License (PAL) is used by carriers that pay to license part of the spectrum. The PA users can bid for a PA license from the FCC, which is usually for a short period (between 3 -5 years) and renewable. PA license (PAL) is also protected from interference from GAA users. It can operate at a frequency up to 70MHz of the 3550 – 3650 MHz spectrum segment within designated geographical areas. During the first bidding process, a prospective applicant can apply for up to two consecutive three-year terms of the Priority Access License (PAL) from the FCC. On a rule of thumb, a maximum of four PALs can be allocated to licenses in a single census tract per time. The spectrum assignment will ensure the availability of the PAL spectrum to a minimum of two licensed users within geographical areas of highest demand. PAL-assigned frequency is not controlled by the SAS and is automatically terminated at the end of its term.

3.2.1.3 General Authorized Access

The General Authorized Access (GAA) spectrum is utilized by unlicensed enterprises for private networks. It can operate at any frequency throughout the 150 MHz bands without interference protection from other CBRS users. GAA uses a licensed-by-rule framework to facilitate the rapid deployment of compliant small-cell devices. It is highly economical for private networks because it reduces administrative costs and license bid burden from the

FCC. However, GAA users can only use FCC-certified CBRS devices, and information such as device ID, operator ID, geographical location, etc., must be registered with the Spectrum Access System (SAS).

The Federal Communications Commission (FCC) requires that Priority Access License (PAL) users cannot interfere with Incumbent users, and General Authorized Access (GAA) users cannot interfere with the Incumbent and PAL users. The Spectrum Access System is responsible for managing interference protection among the three tiers and coordinating spectrum usage of the entrants to protect the incumbents. Based on the nature and critical requirements of the federal Incumbent, the FCC adopted rules to require Environmental Sensing Capabilities (ESCs) to detect the national spectrum used in and adjacent to the 3.5 GHz band. However, to avoid interference issues among the three tiers, FCC proposed the following rules;

- Spectrum allocation is carried out in small geographic and time-based units in order to promote sharing flexibility and expand the entry of the lower tiers.
- Spectrum protection rights are hierarchical, and this implies that the Incumbent users have the highest protection rights.
- The lowest tier, the General Authorized Access (GAA) users, can share any spectrum not used by the Priority Access License PAL and Incumbent users.
- The users of the lowest tier (General Authorized Access) have no interference protection rights.
- The automated process should be employed during the admission of users into the three-tier band to minimize overall cost and time delay and provide seamless access.

3.2.2 CBRS Technical Concept

The CBRS concept consists of the Spectrum Access System (SAS) connected spectrum databases, Environmental Sensing Capabilities (ESCs), Citizens Broadband Radio Service devices (CBSD), End User Devices (EUD), and optionally Domain Proxies and Network Management System (NMS) as shown below;

3.2.2.1 Spectrum Access System

The Spectrum Access System (SAS) is the main technical element of the Citizens Broadband Radio Service (CBRS) and is responsible for managing interference for incumbent users' protection and coordinating the spectrum usage of entrants. SAS ensures that every

Environmental Sensing Capabilities (ESC) operator must have their systems approved, a function controlled by the SAS administrators. It obtains essential information such as registered or licensed commercial users and exclusion zone areas requiring ESC from the Federal Communications Commission (FCC) database. SAS is also responsible for informing other incumbent access users during unplanned or emergency cases of spectrum usage by another federal IA user to avoid interference.

3.2.2.2 Environmental Sensing Capabilities

An ESC consists of one or more commercially operated networks of sensing device-based or Citizen Broadband Radio Service Device (CBSD) infrastructure-based sensors that would be used to detect signals from federal radar systems in the vicinity of the exclusion zones. The ESCs detect incumbent radar activity in coastal areas and near inland military bases adjacent to the 3.5 GHz band. Based on Federal Communications Commission (FCC) rules and the critical requirements of the federal Incumbent, when any Incumbent Access (IA) activity is detected, the ESC communicates that information to the SAS; if it presents a risk of harmful interference, it would order the commercial tier users to vacate the spectrum zone.

3.2.2.3 Citizen Broadband Radio Service Devices

Citizen Broadband Radio Service Devices (CBSDs) are portable base stations or fixed access points that operate under the management and authority of one or more centralized Spectrum Access Systems (SAS) allocated by the Federal Communications Commission (FCC). CBSD information, such as device parameters and identification, operator ID, geographical details, etc., must be registered with the SAS as required by the FCC rule. All the CBSDs must protect the IA users in the band. CBSD can be compared to Mobile Network Operators (MNOs) as both are managed networks. CBSD also includes the domain proxy and network management functionality. Its domain proxy is responsible for the bidirectional processing and routing of information. It performs an intelligent mediation function, while its network management functionality ensures flexible control and interference optimization.

3.2.2.4 End User Devices

SAS dynamically allocates spectrum and maximum power levels to EUDs such as handsets and CBSDs. This assignment is based on the geographic location, licensed sharing area interference environment, and exclusion zones to protect higher-priority users. EUDs must also be registered, authenticated, and easily identified by the SAS based on the FCC rules. As

the Incumbent Access users have primary spectrum rights at all times and in all locations over the Priority Access License (PAL) and General Authorized Access (GAA), all the CBSDs and EUDs must be capable of two-way communications across the entire 3.5 GHz band and changing frequencies or discontinuing operation should be carried out at the direction of the SAS to protect IA.

3.3 Private 5G Network

Digital transformation in the 21st century has brought about the need for advanced network technology to meet up with business-critical requirements such as high network performance, low latency, high reliability, improved security, etc. Over the years, enterprises have implemented technologies like Ethernet, Wi-Fi, LTE, etc., to carry out their business activities. Although these previous technologies met some business needs, such as fixed wireless access, mobile data communication, etc., but couldn't meet up with rapidly growing demands for machine-to-machine communication, robotics, and other mission-critical operations. This business's need is driving the rise of private networks, which enable data to be securely transmitted without going to the public network, therefore, reducing transmission latency, enabling more data access control, and also, delivering highly reliable, secure, and scalable solutions.

The private wireless network is a wide area wireless radio communication network that uses licensed, shared, or unlicensed wireless spectrum for voice and data communication, specifically designed to meet an organization's needs. The growth of the 5G network comes with the rise of private wireless networks. According to the 3rd Generation Partnership Project, it is a non-public network deployed for easy accessibility, reliability, and maintainability. The advent of 5G technology with advanced features of network programmability, ultra-low latency, and network slicing is industrial-strength wireless connectivity required for automation, artificial intelligence, machine learning, and high-speed data processing in the latest Industry 4.0 technology. It also offers improved customization and Quality of Service (QoS), high reliability, security, and predictability, which medium to large enterprises, multinational organizations, and government agencies require for their business needs. Private 5G network enables entities like agriculture, utilities, manufacturing, health, municipalities, factories, etc., to carry out their day-to-day operations at a reduced cost, with better efficiencies, and improve customer satisfaction.

3.3.1 Similarities of private and public 5G network

- Both private and public 5G network uses the same underlying network solutions.
- They utilize the same hardware (5G NR), software, and applications.
- Both make use of the same duplex, modulation, and encoding schemes at the physical layer of their network architecture.
- Both can use the same spectrum, for example, Priority Access License (PAL) in the case of Citizen Broadband Radio Services (CBRS).

3.3.2 Difference between private and public 5G network

Table 3.1 Difference between private and public 5G

Private 5G Network	Public 5G Network
It leverages 5G network architecture for dynamic slicing and dedicated bandwidth.	It is generally provided by Mobile Network Operators (MNOs) to end users and leverages enhanced mobile broadband (eMBB) speeds.
It creates an independent network design and management in an organization (such as an enterprise, factories, industries, etc.) and drives more value toward operating costs.	It uses an existing radio ecosystem for wide-area deployments.
It is a fast-track standalone deployment as there is no dependency on existing 4G infrastructure.	It is primarily non-standalone and leverages existing deployed 4G radio infrastructure as an anchor.
Data is stored and processed locally on the private core network, thereby enhancing security.	Data is processed on the public cloud or network provider's core network.
Spectrum can be acquired from the Priority Access License (PAL) or General Authorized Access (GAA) layer of the Citizen Broadband Radio Services (CBRS) tiers.	Spectrum can only be acquired from the Priority Access License (PAL) layer of the Citizen Broadband Radio Services (CBRS) tiers.

It is dedicated for use in a single or multinational enterprise, organization, or government.	It is used by the public with a population ranging from tens of thousands to millions of subscribers.

3.3.3 Requirements of Private 5G Network

- **High availability:** Private 5G network must provide a downtime of approximately zero percent (R = 0.00000001%). This can be archived by implementing multiple redundant network paths and automated control systems to mitigate network failures, thereby providing a robust solution and maximum service availability to the end users.
- **High reliability:** It must provide URLCC with a data plane latency of 1 ms, mobility interruption time of 0 ms, 99.999% reliability, optimal network coverage, and robust handover functionality for effective packet delivery.
- **Security:** It must comply with the CIA (Confidentiality, Integrity, and Availability) triad policies for information security during data transit and at rest. Its core network should also have an authentication server (Authentication server function) to perform authentication and authorization or an Identity and Access Management (IAM) if deployed in the cloud to ensure end-to-end security and privacy for data, infrastructure, and end users.
- **Interoperability:** Private 5G network infrastructure should be compatible with public 5G networks for easy integration to ensure seamless continuity of service and mobility during critical conditions.

3.3.4 Types of Private 5G Network

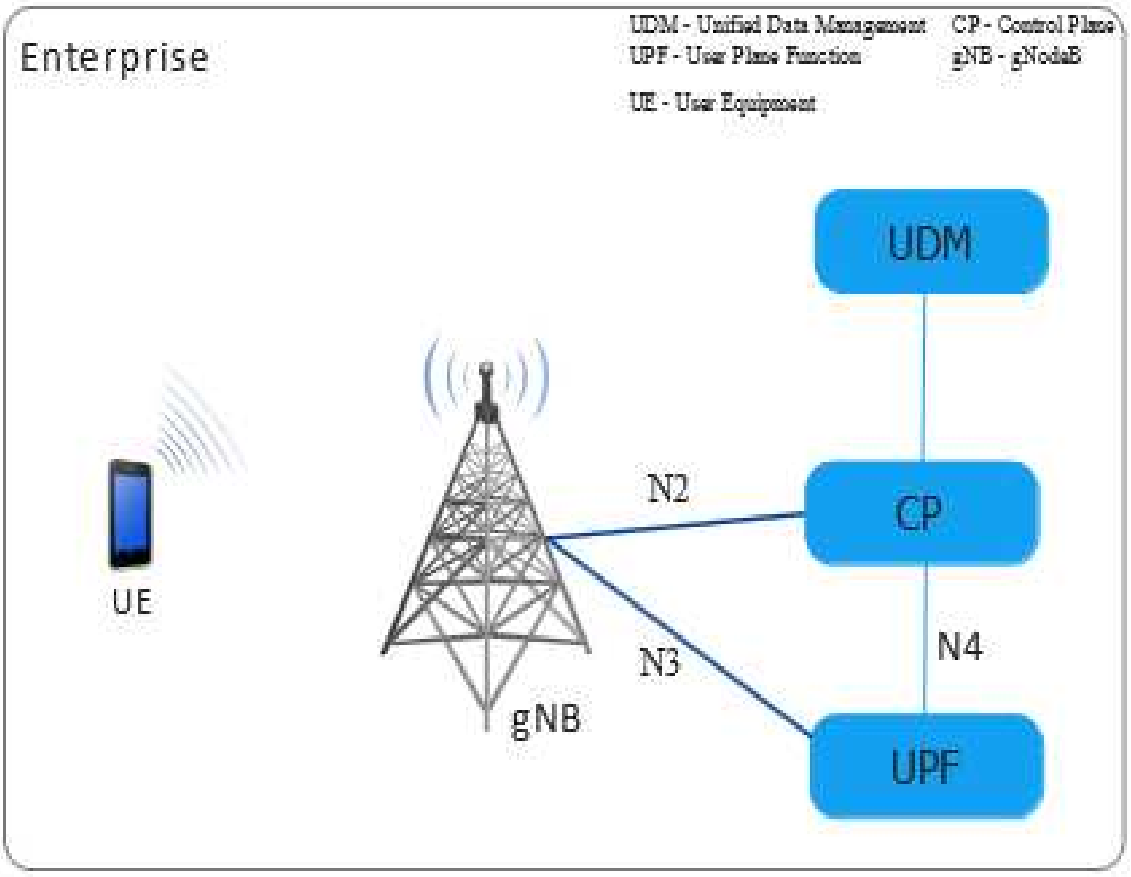
Private 5G networks are divided into two categories based on their mode of deployment as follows:

3.3.4.1 Independent network

This is a solely independent network deployment and is isolated from the MNO's public network as shown in figure 3.1 and 3.2. The enterprise is fully responsible for identifying the spectrum (unlicensed, licensed, or shared) to use, leasing the spectrum from FCC, the installation and configuration of the network infrastructure such as the core network (Unified Data Management, Control Plane, User Plane Function) and radio access network (gNodeB

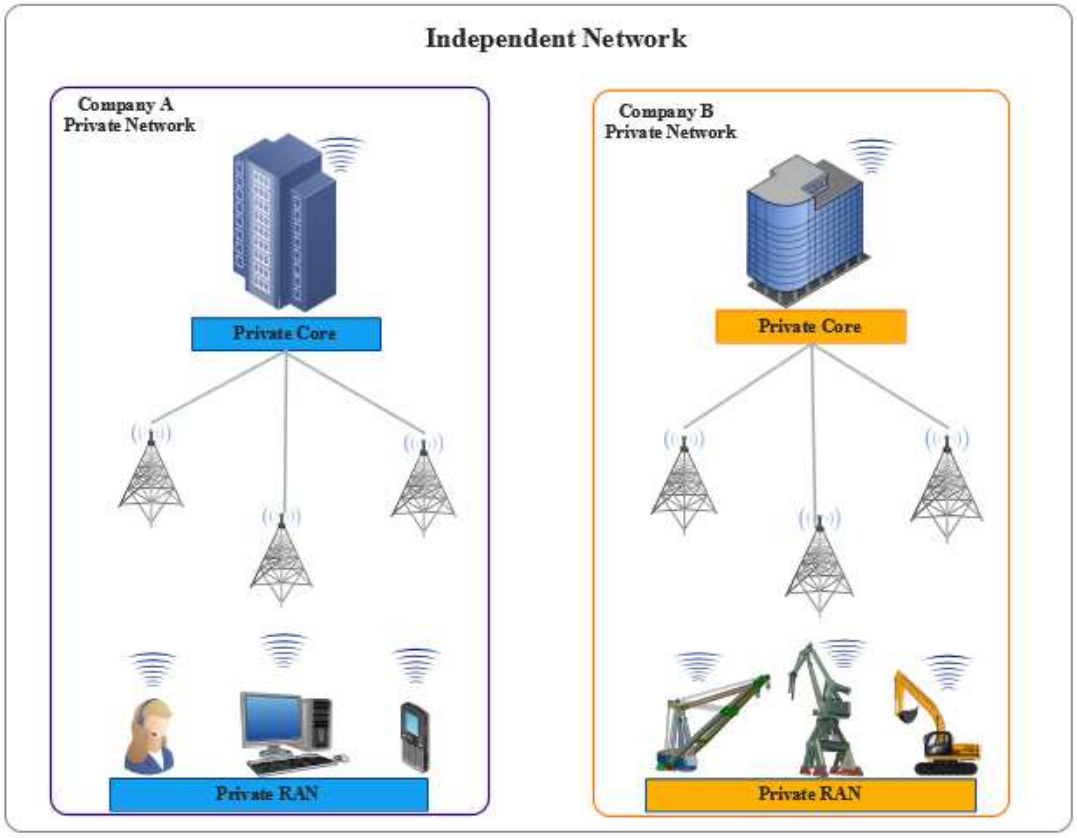
and UE), administration of the subscription users, and also, the maintenance of the network infrastructure and data traffic. This provides additional data privacy as subscription and user information are stored locally and security to the organization's network because its entire network infrastructure is on-premise. In addition, the company's IT team has more control over the network settings, like utilizing its ultra-reliable low latency communications (URLCC) for multi-edge computing, industrial automation, high precision positioning in factories, and other business applications.

Fig 3.1 Independent Private Network Architecture A



Adapted from: Eswaran, S., & Honnavalli, P. (2022). Private 5G networks: a survey on enabling technologies, deployment models, use cases and research directions. *Telecommunication Systems: Modelling, Analysis, Design and Management*, 1–24. https://doi-org.login.ezproxy.library.ualberta.ca/10.1007/s11235-022-00978-z

Fig 3.2 Independent Private Network Architecture B



Adapted from: Eswaran, S., & Honnavalli, P. (2022). Private 5G networks: a survey on enabling technologies, deployment models, use cases and research directions. *Telecommunication Systems: Modelling, Analysis, Design and Management*, 1–24. https://doi-org.login.ezproxy.library.ualberta.ca/10.1007/s11235-022-00978-z

3.3.4.1.1 Advantages of Independent Network

- The enterprise has full control of the network infrastructure deployment, installation, configuration, operation, and maintenance.
- It stores subscription and user information locally in the core network of the enterprise, thereby allowing for an increase in data privacy and security.
- Low operating expenses as there are no subscription charges for users.
- It provides ultra-low latency and autonomous quality of service (QoS) assurance as all network components are on-premise.

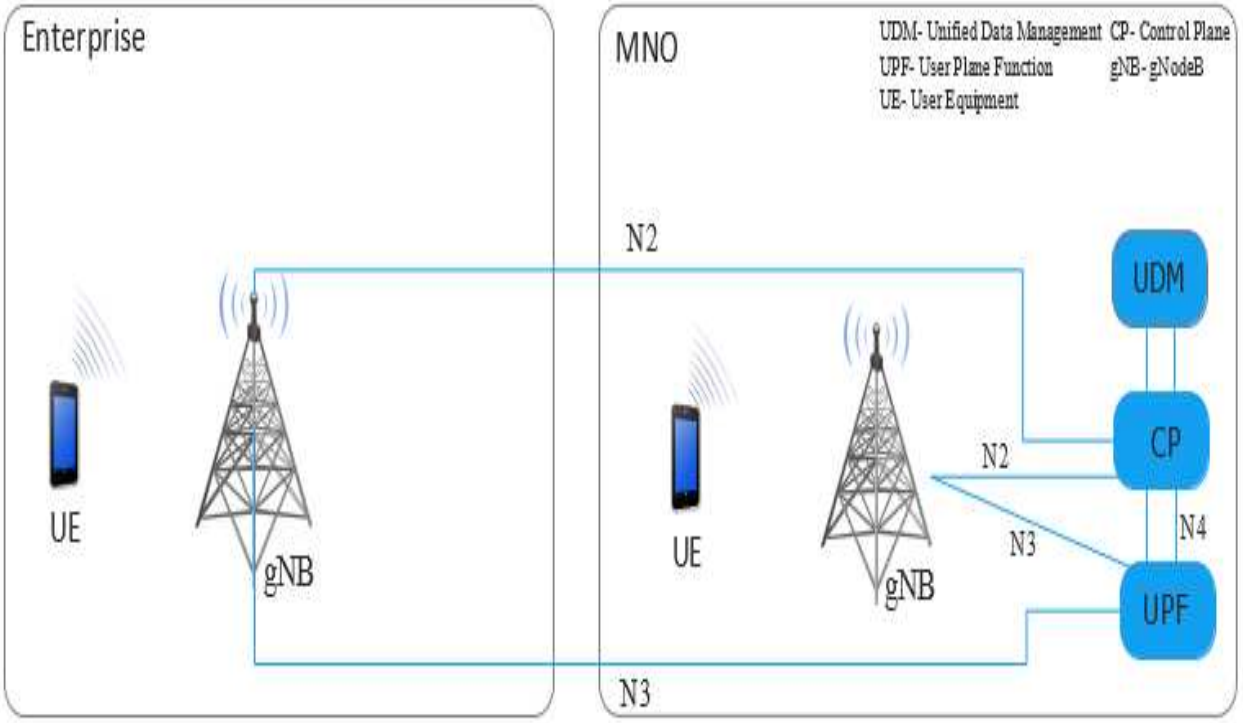
3.3.4.1.2 Disadvantages of Independent Network

- High capital investment for deployment and acquiring dedicated spectrum or license.
- No roaming functionalities.
- It requires highly skilled technical personnel to manage the network infrastructure and operation.

3.3.4.2 Dependent network

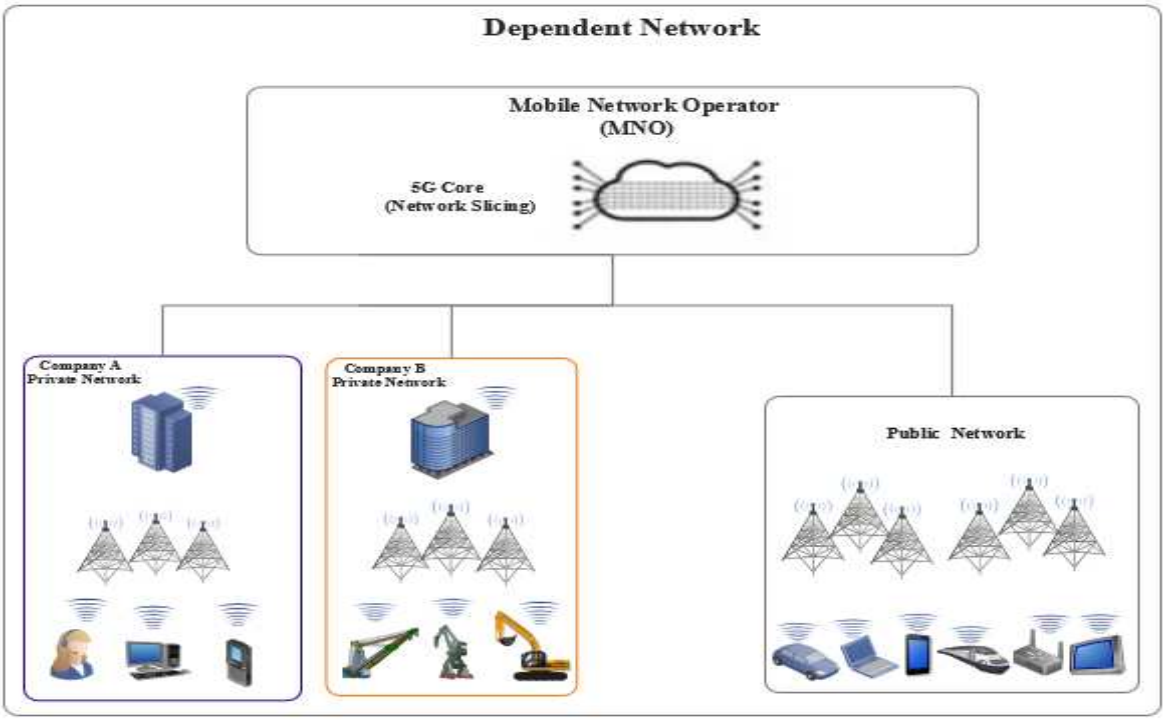
This is a situation whereby a private enterprise or organization uses a leased dedicated spectrum from a Mobile Network Operator (MNO). An MNO could also use network-slicing technology as shown in figure 3.3 and 3.4 to create virtual networks in its physical 5G core network to meet the organization's business needs. The Unified Data Management (UDM), Control Plane (CP), and User Plane Function (UPF) are deployed in the MNO core network. In contrast, the radio access network (RAN or gNodeB) is installed at the enterprise premise. In both cases, the MNO is responsible for installing, configuring, and maintaining the network infrastructure. This results in minimal control of network resources by the private organization and less data privacy as network infrastructure and data are not on the enterprise's business site.

Fig 3.3 Dependent Private Network Architecture A



Adapted from: Eswaran, S., & Honnavalli, P. (2022). Private 5G networks: a survey on enabling technologies, deployment models, use cases and research directions. *Telecommunication Systems: Modelling, Analysis, Design and Management*, 1–24. https://doi-org.login.ezproxy.library.ualberta.ca/10.1007/s11235-022-00978-z

Fig 3.4 Dependent Private Network Architecture B



Adapted from: Eswaran, S., & Honnavalli, P. (2022). Private 5G networks: a survey on enabling technologies, deployment models, use cases and research directions. *Telecommunication Systems: Modelling, Analysis, Design and Management*, 1–24. https://doi-org.login.ezproxy.library.ualberta.ca/10.1007/s11235-022-00978-z

3.3.4.2.1 Advantages of a Dependent Network

- Low capital investment as core network infrastructure such as the UDM (Unified Data Management), CP (Control Plane), and UPF (User Plane Function) reside at the mobile network operators' (MNO) data center. The enterprise could be responsible for the capital cost of shared licensed spectrum, gNodeB, and subscription.
- It leverages an MNO public network for standard roaming functionalities.
- Enterprise leverages managed service as MNOs are responsible for monitoring and maintaining the data traffic.

3.3.4.2.2 Disadvantages of a Dependent Network

- The enterprise does not fully control the network deployment and end-to-end data traffic.
- It stores subscription and user information residing at the MNO core network of the enterprise, reducing data privacy.
- High operating expenses. Enterprise would be required to pay managed service and subscription fees.

Dependency on the Mobile Network Operator (MNO) for signaling and quality of service (QoS).

Chapter 4: Private Wireless Use Cases

4.1 HealthCare

The healthcare industry is one of the industrial sectors private 5G networks tend to address. It will improve access to medical expertise and health care in Canada by providing better medical assistance and services such as health monitoring for early detection and prevention, diagnosis, and emergency intervention. Specialized characteristics of 5G technology, such as ultra-reliable low latency communication (URLCC), high data rate, and reliability, would be utilized by healthcare's IT infrastructure to provide efficient, reliable, secured, and optimal network connectivity. It would enable clinical sensors and IoT devices to communicate with each other via its centralized private core network, would eliminate patient data theft, and provide robust security. Private 5G wireless would allow healthcare providers to monitor, report, analyze, and make quick clinical decisions for patients in acute or critical conditions, irrespective of their physical location or distance from each other. It includes mobile ward rounds, remote consultation, remote surgery, remote diagnostics, and emergency response for diagnostic and therapeutic clinical activities.

4.1.1 Emergency response

5G private networks would improve remote mobile diagnosis by providing high bandwidth, data transfer speed, and high reliability for on-the-move medical services. It would enable health providers, such as doctors, nurses, and medical consultants in the hospital, to receive real-time clinical data of patients in critical condition from the emergency health response team on the field. The patient's data, such as ultrasound images, blood pressure, heart rate, body temperature, and other critical information generated from a remote emergency medical response system, can then be quickly analyzed for proactive decisions for possible treatment in the ambulance before the patient arrives at the hospital.

4.1.2 Remote surgery

This is the process whereby surgeons utilize highly advanced technology to carry out surgical operations remotely. Through digital transformation, specialized surgeons can provide medical services to patients worldwide. 5G network allows surgical operation video streaming and medical imaging data, such as X-ray radiographs, ultrasound images, etc., to be sent in real-time with remote surgery experts without compromising quality.

4.1.3 Remote Diagnosis

Private wireless would improve telemedicine and remote medical services to patients outside clinical environments and distant rural communities. It would help eliminate distance barriers by providing remote diagnoses, such as remote monitoring of a patient's heartbeat, blood pressure, temperature, and other vital signs. 5G enabled wireless sensors can be into remote patient monitoring devices such as Electrocardiogram (ECG) plus stethoscope for capturing patient's heart rate and lung sound, Non-invasive blood pressure (NIBP) monitor for reading blood pressure, glucometer for monitoring patient’s blood sugar level, pulse oximeter for determining a patient’s pulse or blood oxygen level. Remote diagnosis enables healthcare providers to access patients' real-time data for proactive monitoring, analysis, and clinical decisions.

4.2 Industry 4.0

Industry 4.0, also known as the factory of the future, refers to the next generation in the Industrial revolution that utilizes advanced technology to optimize interconnectivity, automation, real-time data processing, machine learning, and other innovations in the manufacturing and industrial sectors. Private 5G wireless provides ultra-reliable low latency communication of less than 10ms, high bandwidth, and reliability to facilitate access point-to-machine communications and device-to-device communications among machinery in manufacturing plants. Compared with previous industrial revolutions, 5G technology would go beyond providing broadband services to end users in customer care, human resources, marketing, and factory floor workers to improving production activities and minimizing operational costs. Private wireless would enable highly sensitive industrial machinery and IoT sensors to operate at high performance, increase reliability, and be more secure. It provides end-to-end connectivity, which results in a predictable performance in the automation of machine-to-machine communication for enhanced productivity across the organization. 5G network technology combined with big data, artificial intelligence, the Internet of Things (IoT), and Edge computing would enable smooth manufacturing, warehousing, and distribution processes in a product life cycle.

A private wireless network offers great benefits for Industry 4.0. The organization has control of the bandwidth distribution and usage because all network infrastructure is on the premise.

Latency is extremely low (< 10ms) as traffic does not transverse across multiple hubs to a remote core network, thereby enabling the rapid processing and analysis of multi-access edge computing and improving data speed for efficient machine-to-machine communication. Furthermore, machines and products are highly secured internally in the on-premise packet core network, such as the health, storage condition, usage level, and location of big data information and analytics.

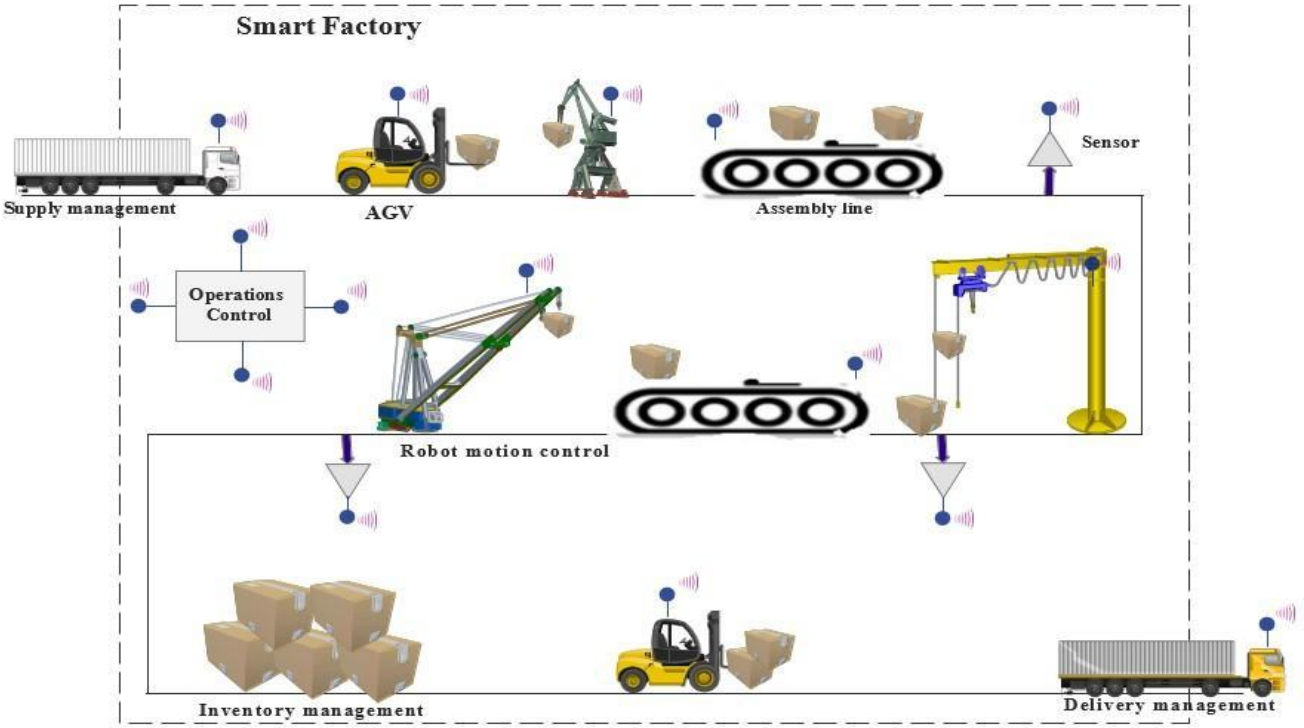
Technologies such as Virtual Reality (VR) and Augmented Reality (AR) are now being implemented in the design of machines and manufacturing equipment to aid machine-to-machine communication, remote or motion control, and monitoring of devices like robots. Some advantages and applications of AR and VR in Industry 4.0 are as follows;

- Augmented Reality and Virtual Reality improve the training and upskilling of staff at various levels of expertise ranging from entry-level employees to experienced senior managers, and reduce training costs.
- It allows engineers and workers to effectively coordinate the assembly of parts by projecting digital work instructions directly onto the work surface during production, reducing production error and increasing productivity, efficiency, and availability of new products to the market.
- It improves worker safety as plant managers can use VR to quickly identify faults in an assembly line and production process and monitor employees' feasibility and task proficiency.
- It simplifies and improves factory floor planning by testing production flows and virtualizing how robots and workers perform their assigned job responsibilities before actual changes are implemented in the real world.
- It drives operational efficiency and improves process flow in the automotive, aerospace, defense, medical, and electronics industries.

The figure 4.1 below illustrates an ideal application of a 5G network in a smart factory. Various examples of how private wireless networks in manufacturing and production environment with applications range from logistics for supply management, networking of Automated Guided Vehicle (AGV), sensors and autonomous transport robots, motion control and coordination of production robots, assembly line control, localization of devices, inventory management to delivery management. Furthermore, private wireless networks meet the communication requirements of Industry 4.0 and are not limited to the Local Area

Network (LAN) of a factory site but can be interconnected across different production sites through a Wide Area Network (WAN) to improve the end-to-end production process.

Fig 4.1 Smart factory based on Industry 4.0 Technology



Adapted from: Trick, U. (2021). *5G : An Introduction to the 5th Generation Mobile Networks*. De Gruyter Oldenbourg.

The following highlights some associated business solutions of 5G private wireless in Industry 4.0:

- It leverages remote maintenance and optimization to increase production uptime and reduce operating costs.
- It would increase operational efficiency, sustainability, and flexibility among connected machinery during production.

- 5G private wireless supports zero manufacturing error in the time-critical optimization process.
- It optimizes value chain processes, logistics control, and asset monitoring by enabling seamless communication across various departments in the organization.
- It expedites innovation by creating value-added services in Industry 4.0

4.3 Smart City

A smart city is an advanced urban geographical area that utilizes technology to gather interconnected information to improve operations and public services across the city. The information is intelligently extracted, relayed, and analyzed to manage assets, services, and resources efficiently. It uses smart technologies such as 5G technology, artificial intelligence (AI), machine learning, cloud computing, application programming interfaces (APIs), and others to address urban challenges, create sustainable infrastructure, improve operational efficiency, promote economic growth and development, and also, improve citizen welfare.

Private wireless networks are projected to overcome smart cities' challenges by providing high data mobility, ultra-reliable and low latency communication between modern assets such as smart lighting, surveillance cameras, intelligent traffic control, etc., and backend infrastructures for data analytics. Strategic environmental initiatives, highly effective and functional public transportation systems, and infrastructural design based on technology are a few of the characteristics used in determining a smart city. The following highlights some of the use cases of private wireless networks in smart cities:

4.3.1 Traffic management

5G private wireless can improve traffic congestion control by easing the automation of large volumes of sensor data collection and mobility of data traffic. It allows for fast wireless interconnectivity of IoT infrastructures and sensors. Therefore, empowering mission-critical applications such as road traffic patterns, air quality, electric energy usage, parking meters, and so on to be monitored and managed effectively. The table 4.1 below illustrates the average traffic congestion level in 2021 and the hours lost per year at some of the busiest cities in Canada.

Table 4.1 Canada traffic ranking by city

COUNTRY RANK	CITY	TIME LOST PER YEAR	CONGESTION LEVEL 2021	CHANGE FROM 2019	CHANGE FROM 2020
1	**Vancouver**	75 hours	**33%**	↓ 6%	↑ 3%
2	**Montreal**	55 hours	**24%**	↓ 5%	↑ 4%
3	**Toronto**	55 hours	**24%**	↓ 9%	↑ 2%
4	**London**	46 hours	**20%**	↓ 3%	↑ 2%
5	**Halifax**	43 hours	**19%**	↓ 6%	↑ 2%
6	**Winnipeg**	43 hours	**19%**	↓ 3%	↑ 2%
7	**Quebec**	41 hours	**18%**	↓ 4%	↑ 4%
8	**Ottawa**	41 hours	**18%**	↓ 11%	↓ 1%
9	**Calgary**	32 hours	**14%**	↓ 4%	↑ 1%
10	**Hamilton**	32 hours	**14%**	↓ 5%	↑ 2%
11	**Edmonton**	29 hours	**13%**	↓ 3%	0%
12	**Kitchener-Waterloo**	27 hours	**12%**	↓ 4%	0%

Increase in congestion, decrease in congestion, no change in congestion.

Adapted from: *Canada traffic report: TomTom Traffic Index*. report | TomTom Traffic Index. Retrieved February 14, 2023, from https://www.tomtom.com/traffic-index/canada-country-traffic/

Private wireless network solutions can be utilized by each province's traffic management in Canada and deployed across busy cities and municipals to minimize the traffic congestion level and lost time drastically. For example, LED Roadway Lighting Ltd, a Canadian clean technology company headquartered in Nova Scotia, designed a solution that allowed cities and municipals to monitor traffic and minimize traffic congestion and accidents. This solution uses a Toolless Sensor Platform (TSP) radar with an embedded Low Power Wide Area (LPWA) module installed on existing

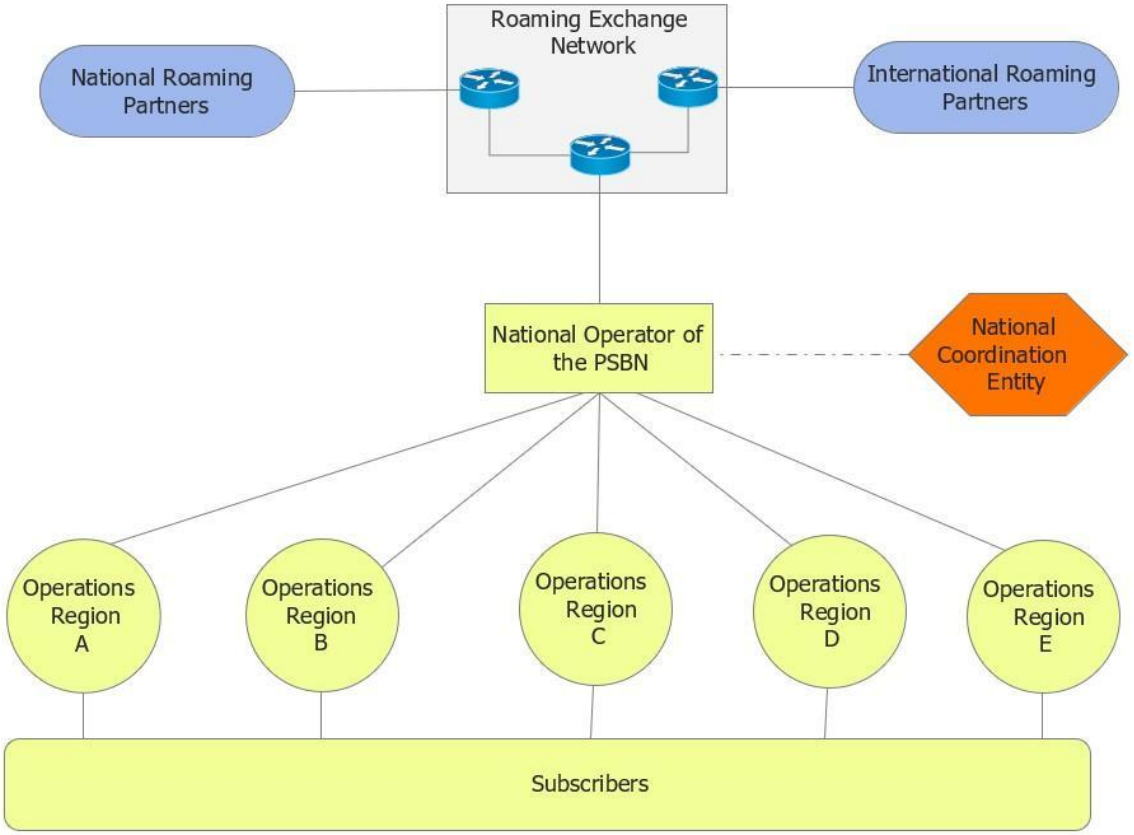
street light infrastructure to monitor and relay real-time traffic volume and speed data to the cloud platform for analysis and city administration.

4.3.2 Security and Public Safety

Private wireless networks can be used by public safety personnel and emergency responders to access and share critical information reliably and also communicate with each other during day-to-day operations, emergencies, weather-related incidents, and natural disasters. For example, in Canada, integrating a private wireless network in the public safety broadband network (PSBN) by Public Safety Canada, Communications would enhance communication capabilities, emergency prevention, and response and improve community safety. Firstly, a private wireless network would greatly improve 911 emergency service beyond voice call service to receiving enhanced insight and incident information such as high-resolution images, location data, and high-definition video through digitally-enabled channels. PSBN principles such as interoperability, sustainability, coverage, mission-critical service delivery, network access always, security, etc., can be easily archived by deploying and operating private network solutions.

Secondly, the CBRS spectrum can be licensed by FCC and used across the five operation regions across Canada to provide private wireless network solutions. According to the figure 4.2 and table 4.2 below, public safety organizations such as Royal Canadian Mounted Police (RCMP), Canada Security Intelligence Service (CSIS), and others can communicate and share data-intensive information. Each operation region can operate as a stand-alone private wireless network with a 5G core network on-premise to improve data speed due to low latency communication. The central location can connect the five operation regions across Canada for national operation, coordination, roaming, and switching functions for inter-regional communications.

Fig 4.2 Private Wireless Network Solution for PSBN, Canada



Adapted from: Canada, P. S. (2022, July 20). *A Public Safety Broadband Network (PSBN) for Canada*. Public Safety Canada. Retrieved February 18, 2023, from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-psbn/index-en.aspx

Table 4.2 PSBN organization and operations region

Subscribers	Public safety agencies	Royal Canadian Mounted Police
		Canada Security Intelligence Service
		Canada Border Services Agency
		Correctional Service of Canada
		Parole Board of Canada
	Public safety review bodies	Civilian Review and Complaints Commission for the RCMP
		Office of the Correctional Investigator
		RCMP External Review Committee
	Other units	Canadian Cyber Incident Response Centre
		National Search and Rescue Secretariat
Operations Region	A	Atlantic (Newfoundland and Labrador, Prince Edward Island, Nova Scotia, New Brunswick)
	B	Quebec and Nunavut
	C	Ontario
	D	Manitoba, Saskatchewan, Alberta, Northwest Territories
	E	British Columbia and Yukon
National operator	Private Wireless Network Solution using Citizen Broadband Radio Service (CBRS)	Public Safety Canada, Communications

Roaming Exchange Partners	External Gateways	Mobile Network Operators (MNOs)
		Publicly Switched Telephone Network (PSTN)

4.4 Transportation and Logistics

4.4.1 Smart Airport

Business stakeholders at both International and local airports must keep advancing their operational and service efficiencies to meet growing customer demands. Smart airports depend on intelligent digital infrastructure to enable highly efficient, sustainable, and autonomous operations. The aviation industry can adopt private wireless networks to provide solutions for both the land and airside at airports. It would enable secure, high-performing, and seamless analytics of real-time data with connected assets, airport staff, and customers. Ultra-high-speed wireless connectivity, high reliability, and low latency of 5G technology guarantee wide coverage, bandwidth capacity, and scalable QoS (Quality of Service) for connected aircraft, telemetry upload, download, and analytics of terabytes of data during the flight, digital operations, and mission-critical communications.

A private wireless network would enhance situational awareness in an airport. For example, vehicles can be equipped with wireless cameras for real-time visibility of first responder vehicles on the runway at the Airport Operations Center (APOC), wireless sensors for real-time visibility of upcoming flights and aircraft that require de-icing during extreme weather conditions, and wireless body cameras for security personnel for real-time video streaming to airport security control office. It will have a great positive impact on the operational efficiency and automation of routine airport activities such as airplane embarking and disembarking processes, baggage loading, scanning, processing and offloading, asset tracking, and management, reduce ground handler labor costs, and also lower overall service turnaround times. Private 5G networks help airports minimize complete dependency on mobile network operators (MNOs, or network service providers for digital transformation.

They also give the IT personnel total control of their network infrastructure to achieve reliable, secured, and highly efficient wireless connectivity.

4.4.2 Smart port

Shipping ports are a prime use case for private wireless networks because of the large number of trucks and containers in constant motion. With private wireless solutions, few fixed access points such as gNodeB/ Radio access networks can be strategically deployed at different port areas for full coverage compared with hundreds of access points (Wi-Fi) deployed in the past. Port authorities can purchase license 3,500 MHz bands of the Citizen Broadband Radio Service (CBRS) spectrum through the General Authorized Access (GAA) from Federal Communications Commission (FCC) to enable coverage of entire seaport facilities across Canada with adequate penetration power for metallic objects such as containers, cranes, ships, and cargo handling equipment without signal loss and interference. Deploying this solution whereby the mobile core EPC is on-premise allows for predictable connectivity among IoT devices for seamless equipment monitoring, asset tracking, and routing in a controlled environment transportation hub. In addition, private wireless network promises would enable next-generation port terminal automation of remote-controlled container handling equipment such as straddle carriers and other automated guided vehicles (AGV) to improve operational efficiency and productivity.

4.4.3 Logistics

This refers to the centralized facilities such as warehouses, distribution, and fulfillment centers for shipping, storage, sorting, packaging, and repackaging of commercial and retailer products, and conveyed with trucks, trains, and ships. Logistic environments are highly dynamic areas with the constant movement of new products and huge inventory management of existing goods that require ultra-reliable and low latency connectivity for asset tracking, ruggedized tablets, push-to-talk handheld devices, automated guided vehicles, and other automated infrastructure that require fast network connectivity. A private wireless network can improve the way networked information and sensors communicate. It drives rapid data analytics to optimize the scheduling and packaging of goods, improve turnover times and reduce shipment errors, and enable predictive maintenance in logistic environments, thereby saving costs.

Chapter 5: Private Wireless Network Challenges

The demand for higher network bandwidth, privacy, data security, and low-latency communication is increasing rapidly. The private wireless network market was valued globally at USD 1.38B in 2021 and is forecasted to multiply at a compound annual growth rate (CAGR) of 49% till 2030. It is now being deployed by governmental agencies, enterprises, the manufacturing industry, healthcare, etc., in North America and Canada. For example, Detour Lake, a subsidiary of Kirkland Lake Gold, deployed a private wireless network in its remote open pit mine in northern Ontario. It helps create a safer work environment for employees, clients, contractors, and stakeholders. However, the technical, regulatory, cost, integration, etc. challenges are essential limiting factors to be considered. The key challenges associated with private wireless network deployment are as follows;

5.1 Regulatory Challenges

Government regulation of spectrum availability and usage is a significant challenge in using private wireless network solutions. More spectrum is required to improve 5G network throughput across enterprises. 5G networks can use spectrum from the low band (< 1GHz), mid-band (1 – 6 GHz), and high-band (> 6GHz), but its usage is regulated by Federal Communications Commission (FCC) in the United States. Unfortunately, despite the flexibility of using shared and unlicensed frequency bands for 5G networks, most frequency band organizations can use still falls under the licensed spectrum. In Canada, the federal government, through the Innovation, Science and Economic Development (ISED), regulates access to spectrum and radio frequency (RF) devices. At the same time, the Canadian Radio-Television and Telecommunications Commission (CRTC) supervises and regulates telecommunications and broadcasting in the public interest.

The Canadian government has always relied on using auctions for spectrum allocation and finally gets allocated to the highest financial bidders. In 2021, Canada raised $7.2B in a 3.5GHz auction for 5G, with the majority share from telecommunication giants such as Rogers Communication ($2.7B), Bell Mobility ($1.7B), Telus ($1.5B), and other large enterprises. However, the limited available spectrum poses a significant threat to most enterprises as it tends to be uneconomical to purchase spectrum from FCC due to its high auction cost. Realistically, enterprises must rely on network slicing provisioning or buy a portion of the spectrum (shared spectrum) from managed network operators (MNOs) to implement their private wireless network solutions. However, an alternative option of utilizing unlicensed spectrum in 5G technology has created more possibilities for private wireless network deployments. In addition, it will give enterprises more control to effectively administer and manage their network security, performance, and application.

5.2 Integration Challenges

Integrating various requirements, spectrum assets, technological components, platforms, and applications for optimal performance is one of the main challenges facing the deployment of the private wireless network. Firstly, private 5G network planners must decide during the design phase if the wireless solution will be an independent private network, that is, be acquired and seen as part of an enterprise's asset, or as a dependent private network service proffered by a managed network operator (MNO). Secondly, if deployed as a dependent private wireless solution, 5G network components which include network slice orchestrator, 5G Radio units, disaggregated and virtualized 5G Core containerized Network Functions (CNFs), Time-sensitive Networking (TSN) enable XHaul routers, virtualized distributed units (DUs) and Centralized units (CUs), and Multi-access Edge Compute (MEC) applications are designed by different vendors. Therefore, they need to be integrated end-to-end to deliver the required performance. Moreover, dependent private networks require several heterogeneous networks and applications such as RAN, core network, cloud, and core transport resources to be well configured to interoperate. Finally, private wireless network integrators must design, build, and test private 5G networks based on the enterprise capital expense budget to meet the organization's specific performance and service requirements.

5.3 Technical Challenges

The deployment of the private wireless network for enterprises depends on the availability and technicalities of the available spectrum. 5G network uses a higher frequency range to

meet highly demanding data availability, throughput, reliability, and low latency. However, the coverage range of radio waves propagated at these higher frequencies is smaller, which is a significant challenge. Large enterprise environments such as ports, factories, and mining with thousands of square miles would require several radio access networks (RAN) and extra repeaters to be placed at strategic locations for full 5G coverage and must be factored in during the planning phase.

5.4 Operational Challenges

A private 5G network can be deployed as a dependent or independent wireless solution. If deployed as a dependent private wireless, more skilled professionals are required at the managed network operator (MNO) to orchestrate the network slices or shared network. This complex heterogeneous network infrastructure which consists of the network edge, transport, cloud, and other layers, needs to be carefully segmented between different enterprises to ensure a high level of data security, privacy, quality of service (QoS), speed, and low latency. In addition, traffic flow synchronization, inter-sliced network performance, and continuous service demand changes are also essential factors to consider during operation.

If deployed as an independent private 5G network, a workforce such as skilled network engineers, software developers, programmers, and other IT professionals must implement private wireless network solutions from planning to the operational phase. In addition, critical measures such as fault detection, root cause analysis, auto-scaling, and fast service restoration must be factored in to maximize network reliability and availability. Unfortunately, most enterprises need more skilled professionals in their current workforce, leaving them with the option of either continuously sorting for talented personnel in the job market or training the current technology workforce.

5.5 Security Challenges

Previous generations of the Industrial revolution relied on wired technology for their day-to-day business operations, were often isolated from the Internet, and were less prone to network attacks. However, enterprise network attacks became prominent in Industry 3.0 when wireless technology was introduced, forcing businesses to protect their data and network with robust security tools such as firewalls, Intrusion prevention detection systems (IDPS), access control, antivirus software, etc. Furthermore, the advent of 5G technology in

the private wireless network also comes alongside its security challenges with network attacks in the form of physical versus logical and local versus remote attacks.

Physical attacks involve hacking network devices such as routers, switches, and firewalls and manipulating their physical characteristics and performance. As a result, it disrupts network infrastructure, manipulates enterprise critical data, or can cause physical harm to humans. On the other hand, logical attacks exploit vulnerabilities such as outdated antivirus, malicious software, and misconfigured firewall in the network security implementation. Though the ease of automation features in the 5G network has many advantages, it also has some downsides. For example, threat actors and hackers can automate bot scripts to perform distributed denial-of-service attacks on many network devices. Therefore, confidentiality, integrity, and authentication of network hardware, software, and data are crucial in the design of a private wireless network. In addition, the network security architecture should support low latency, scalability, efficiency, and communication requirements for enterprise applications. Hence, local and remote security attacks should be carefully considered when implementing a private wireless network.

Chapter 6: Conclusion

Private wireless networks are dedicated 5G networks that greatly benefit enterprises, businesses, governmental organizations, and agencies. Being a new technology, it is gradually gaining propulsion as government spectrum regulators such as Innovation, Science and Economic Development (ISED) in Canada and Federal Communications Commission (FCC) in the United States allocate additional spectrum to help businesses deploy, operate and maintain their private wireless networks. It is a ground-breaking and transformative solution for the 3rd Generation Partnership Project (3GPP) mission-critical applications such as healthcare, transportation, Industry 4.0, smart cities, etc. A private 5G network is relatively new in the wireless technology market, and research is still ongoing on the best architectural, deployment, integration, and operational methods. As a result, most private wireless network deployments at large organizations in Canada and North America are deployed as a dependent private network via network slicing and managed by Mobile Network Operators (MNOs). It is forecasted that private 5G network deployment as an Independent private network will be more practicable as government regulators allocate more spectrum; for example, Innovation, Science and Economic Development (ISED) in Canada plan to auction the 3800 MHz in 2023.

This project report presents a brief history of cellular wireless technology from the first generation to the Fourth generation, an overview of 5G technology and private wireless networks, use cases, and the challenges facing private wireless network deployment. In addition, this paper discussed the relationship between 5G technology and private 5G network extensively. Therefore, it should convey adequate knowledge for 5G network professionals, researchers, and academicians interested in 5G technology, private wireless networks, use cases, and challenges.

In summary, the private wireless network presents an opportunity to enhance the digital transformation of various industrial sectors by delivering higher data speed, availability, privacy, ultra-low latency, and security. Furthermore, this improved wireless solution performance will enable new use cases and technology applications and create a differentiation strategy among large organizations, thereby fostering business competition in the vertical market.

References

[5G-mmtc]smart city solution: Solution - gigabyte global. GIGABYTE. (n.d.). Retrieved October 29, 2022, from https://www.gigabyte.com/Solutions/mmtc

5G is here: How will this impact emergency communications? - CISA. (n.d.). Retrieved February 21, 2023, from https://www.cisa.gov/sites/default/files/publications/22_0629_NECP_Webinar_Technology_5G_Slide_Presentation_508C.pdf

Alexiou, A. (2017). *5G wireless technologies*. The Institution of Engineering and Technology.

Bhatia, A. (2021, May 4). *How is a Private 5G Network Different from a Public 5G Network?* Retrieved from: https://www.samsung.com/global/business/networks/insights/blog/0503-how-is-a-private-5g-network-different-from-a-public-5g-network/

Canada, P. S. (2022, July 20). *A Public Safety Broadband Network (PSBN) for Canada*. Public Safety Canada. Retrieved February 17, 2023, from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-psbn/index-en.aspx

Canada traffic report: TomTom Traffic Index. report | TomTom Traffic Index. Retrieved February 14, 2023, from https://www.tomtom.com/traffic-index/canada-country-traffic/

Clint, S., Daniel, C. *3G Wireless Networks* (McGraw-Hill, 2002). https://www-accessengineeringlibrary-com.login.ezproxy.library.ualberta.ca/content/book/9780071363815

Clint, S., Daniel, C. 2014. *Networks: Design and Integration Wireless for LTE, EVDO, HSPA, and WiMAX*. 3rd ed. New York: McGraw-Hill Education. https://www-accessengineeringlibrary-com.login.ezproxy.library.ualberta.ca/content/book/9780071819831

Corporation, C. (n.d.). *The top 3 challenges of private 5G*. Ciena. Retrieved February 27, 2023, from https://www.ciena.com/insights/articles/2022/the-top-3-challenges-of-private-5g

DeGrasse, M. (2020, May 21). *Transportation hubs likely to deploy private wireless networks using CBRS*. Fierce Wireless. Retrieved February 18, 2023, from https://www.fiercewireless.com/wireless/transportation-hubs-expected-to-deploy-private-networks-using-cbrs

Elena Muller, M. P. H. (2022, November 2). *7 common remote patient monitoring devices*. HRS. Retrieved February 19, 2023, from https://www.healthrecoverysolutions.com/blog/7-common-remote-patient-monitoring-devices

Eswaran, S., & Honnavalli, P. (2022). Private 5G networks: a survey on enabling technologies, deployment models, use cases and research directions. *Telecommunication Systems: Modelling, Analysis, Design and Management*, 1–24. https://doi-org.login.ezproxy.library.ualberta.ca/10.1007/s11235-022-00978-z

Ghonge, M., Mangrulkar, R. S., Jawandhiya, P. M., & Goje, N. (2021). *Future Trends in 5G and 6G : Challenges, Architecture, and Applications* (First edition.). CRC Press.

Innovation, S. and E. D. C. (2022, June 30). *Government of Canada announces spectrum auction rules supporting high-quality and affordable wireless services.* Canada.ca. Retrieved February 28, 2023, from https://www.canada.ca/en/innovation-science-economic-development/news/2022/06/government-of-canada-announces-spectrum-auction-rules-supporting-high-quality-and-affordable-wireless-services.html

Liveable cities enables Smart City Traffic Management via Street Light Infrastructure. Sierra Wireless. (2022, June 14). Retrieve d February 14, 2023, from https://www.sierrawireless.com/resources/customer-stories/smart-city-traffic-management/

Juha, K. (2014). *Introduction to 4G Mobile Communications*. Artech House.

Marshall, P. (2017). *Three-Tier Shared Spectrum, Shared Infrastructure, and a Path to 5G*. Cambridge: Cambridge University Press. doi:10.1017/9781108165020

Patrick, M., Ãmer, B., Olav, Q., & Mauro, B. (2018). *5G System Design : Architectural and Functional Considerations and Long-Term Research*. Wiley.

Sohul, M., Yao, T., & Reed, J. "Spectrum access system for the citizen broadband radio service," in *IEEE Communications Magazine*, vol. 53, no. 7, pp. 18-25, July 2015, doi: 10.1109/MCOM.2015.7158261.

Trick, U. (2021). *5G : An Introduction to the 5th Generation Mobile Networks*. De Gruyter Oldenbourg.

Usankin, A. (2021, March 25). *The demand for Private 5G is there. here are 3 challenges standing in its way*. The SHI Resource Hub. Retrieved February 26, 2023, from https://blog.shi.com/next-generation-infrastructure/demand-challenges-of-private-5g/

WP 5G for connected industries and automation Korrektur 01.11.18 +logos. (n.d.). Retrieved February 28, 2023, from https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2019/Maerz/5G_for_Connected_Industries_and_Automation/WP_5G_for_Connected_Industries_and_Automation_Download_19.03.19.pdf