UNIVERSITY OF ALBERTA

Smart city private wireless network use cases & challenges

MINT Research Project
Sana Salman 1712361
Project Supervisor: Shahnawaz Mir

Date: February 26, 2023
Version: 1.3

Document Status:

Title:	Smart city private wireless network use cases & challenges			
Status:	☐In progress	☒Reviewed	☒Validated	☒ Approved
Owner:	Sana Salman, University of Alberta			
Author:	Sana Salman			
Document Type:	Research Project			
Version:	1.3			
Release Date:	02/26/2023			
Supervisor:	Shahnawaz Mir			
Approval/Reviewer:	Shahnawaz Mir			

Document History:

Version	Date	Changes Made
0.1	September 07, 2022	Draft version creation
0.2	September 14, 2022	Draft updates
0.3	September 26, 2022	Draft update
0.4	October 10, 2022	Review comments update
0.5	October 21, 2022	Draft update
0.6	October 28, 2022	Draft update
0.7	November 11, 2022	Review comments update
0.8	November 18, 2022	Draft update
0.9	December 09, 2022	Draft update
1.0	January 11, 2023	Review comments update
1.1	January 18, 2023	Review comments update
1.2	February 08, 2023	Review comments update
1.3	February 15, 2023	Review comments update

References:

References
https://www.cisa.gov
https://www.3gpp.org
https://www.itu.int
https://www.ericsson.com/
https://www.verizon.com/
https://www.qualcomm.com/
https://www.mdpi.com/
https://telecoms.com/
https://iotmktg.com/
https://www/cisco.com/
https://futurenetworks.ieee.org
https://www.etsi.org
https://www.nokia.com
https://www.thalesgroup.com/
https://www.gsma.com
https://5gobservatory.eu/
https://www.policytracker.com
https://www.fcc.gov/
https://www.mckinsey.com/
https://www.rcrwireless.com
https://www.state.gov
https://www.csis.org/
https://www.faa.gov/
https://www.ascm.org/
https://www.researchgate.net
https://www.bell.ca
https://www.telus.com
https://www.rogers.com
https://www.publicsafety.gc.ca/

Glossary:

Term	Definition	Term	Definition
AI	Artificial Intelligence	IoT	Internet of Things
OAN	Open Access Network	ICT	information and communication technologies
LTE	Long-Term Evolution	5G	fifth-generation technology standard
WRC	World Radiocommunication Conferences	ITU	International Telecommunication Union
SMARTER	Study on New Services and Markets Technology Enablers	eMBB	enhanced Mobile broadband
URLLC	Ultra-Reliable Low Latency Communications	LPWAN	Low Power Wide Area Networks
VR	Virtual reality	ROI	Return on Investment
ICT	Information and communication technologies	IEEE	Institute of Electrical and Electronic Engineers
1G	First Generation	2G	Second Generation
GPRS	General Packet Radio Service	SMS	Small messaging services
WAP	Wireless Application Protocol	MMS	Multimedia messaging services
EDGE	Enhanced Data rates for GSM Evolution	3G	Third Generation
HSDPA	High-Speed Downlink Packet Access	UMTS	Universal Mobile Telecommunication System
3GPP	3rd Generation Partnership Project	4G	Fourth Generation
WiMAX	Worldwide Interoperability for Microwave Access	ITU	International Telecommunication Union
LTE	Long Term Evolution	5G	Fifth Generation
SBA	Service-Based Architecture	PCF	Policy Control Function
UDM	Unified Data Management	SMF	Session Management Function
Li-Fi	Light Fidelity	OWC	Optical Wireless Communications
NSA	Non-Standalone	LED	Light-Emitting Diodes

MIMO	Multiple Input, Multiple Outputs	mmWave	Millimetre wave
TDD	Time-Division Duplexing	FDD	Frequency Division Duplexing
M-IoT	Massive Internet of Things	5G NR	Fifth Generation New Radio
MEC	Multi-access Edge Computing	DU	distributed units
CU	centralized units	CISA	Cybersecurity and Infrastructure Security Agency
AI	Artificial Intelligence	ML	Machine Language
5G RAN	5G Radio Access Network	UE	User Equipment
UNI	User Network Interface	NNI	Network to Network Interface
SIM	subscriber identity module	V2X	Vehicle-to-Everything
ADAS	advanced driver assistance systems	ITS	Intelligent transportation system
AR	Augmented Reality	RAS	Robotic-assisted Surgery
ALPR	Automated License Plate Recognition	ANPR	Automatic Number Plate Recognition

Table of Contents

Table of Figures

1. Overview

The population of urban regions is growing by about 55% and will reach 68% in 2050, according to the UN. For the benefit of their citizens, companies, and visitors, municipalities are investing in technology to increase safety, mobility, sustainability, and efficiency.

Municipalities needed sustainable infrastructure due to this related growth and the resulting global demographic shift to guarantee future-proof cities. In addition, municipalities are undergoing a digital transformation and evolving into intelligent cities as they boost connectivity, advancing services for companies and citizens to designate cities as places that will not only improve quality of life but also guarantee sustainability, security, and safety, as well as draw in more tourists and investors.

The sustainable or prospective concept of smart cities demands outstanding performance and consistent connectivity. In most cases, fiber-based connections between intelligent cities and conventional telecommunications and internet service providers are made. The Internet of Things (IoT) is rising exponentially; there are more connected devices, and advances in communication technology, like 5G, can support a path forward with a privately owned network that can connect people, sensors, and smart objects by utilizing advanced technology. A few examples of the extensive real-time communication required for managing this rise in devices in digital cities include the expanding traffic management and rerouting systems, an intelligent surveillance security system that reduces crime with real-time control, and autonomous and connected vehicles.

Efficient urban planning while increasing population day by day in urban areas requires effective initiatives that include advanced traffic management, smart security, optimization of traffic routes, control of connected and autonomous vehicles, advancement in the mobilization of security, police, ambulance or firefighters, and many environmental initiatives require massive extensive data management with high-speed connectivity and low latency that in some extent possible with standard fiber connectivity but not efficient, sustainable and future proving.

1.1 Aims and objectives.

The increasing demand for connected devices using advanced digital technologies AI, IoT, big data, and augmented and virtual reality requires open access networks in smart cities and demands high speed, low-latency data transmission, and ubiquitous connectivity. The low-latency data transmission and ubiquitous connectivity for real-time big-data communication require a private wireless network to transform the traditional infrastructure. This shift will allow the use of advanced digital technologies and also helps to achieve the benefits of optimizing cost, public services, sustainable future-proof cities, advanced security, investors, and maintaining the companies with limited investment.

A solid private wireless network is the central pillar of a future-proof smart city that connects the city devices with low-latency data transmission, high performance, reliable data protection, and robust and secure communication.

This research focuses on the challenges of adopting the private wireless network in smart cities in contrast to its different deployment scenarios. The study also includes use cases that will require extensive data management for enhanced broadband to high data rates. IoT with ultra-high density or critical control devices/sensors that requires strong security, high reliability, or ultra-low latency.

The key driver behind this is the spectrum for the private wireless network, and it is a big challenge to adopt private wireless technology due to its limitations. The research also includes overcoming the spectrum's limitations that enhance security and eliminate health concerns by reducing the radio frequencies in some use cases.

In addition, this research emphasizes the transformation of technology and how smart cities need to adopt private wireless networks that will justify the current demand and sustainable infrastructure to ensure future-proof cities.

2. Open access networks in smart cities and private wireless usage benefits

2.1. Smart City Overview

The city may be considered a service organization with citizens as its customers - it provides services to its citizens as there is a demand for a more innovative, effective, efficient, and sustainable city. Pushing the collective intelligence of cities onward can improve the ability to forecast and administer urban flows and integrate the dimensions of a regional agglomeration's physical, digital, and institutional spaces. Urban development and improvement of the city have been bending towards technology. Smart cities are using different information and communication technologies (ICT).

Solutions characteristically include various aspects of a city ecosystem, such as smart infrastructure, intelligent operation, competent service, smart industry, innovative education systems, or smart security systems.
Cities are transforming from digital cities to intelligent ones that are more technology-oriented and equivalent to smart city concepts. A town becomes "smart" when it is instrumented, interconnected, adaptive, autonomous, self-learning and self-repairing. Elements of its infrastructure and facilities are digitally connected and optimized using ICT to deliver services to its citizens and other stakeholders.

2.2. Open access networks in smart cities

The central pillar of the smart city is digitally connected infrastructure, fiber optic infrastructure, which is commonly the first step towards a city's digitalization. The fiber optic infrastructure typically adopts the Open Access Network (OAN) model to become technology-oriented, equivalent to smart city concepts.

In telecommunications, a business model of horizontally layered network architecture that separates the physical access of networks from service provisioning define as an Open Access Network (OAN). The same model OAN will be used by several different providers that may or may not share the investment or the maintenance cost. Open access networks are the feasible way of deploying next-generation broadband networks compared to other techniques. Without the OAN standard, it is hard to acquire a sufficient Return on Investment (ROI) for service providers to cover the high costs associated with trenching, right-of-way encroachment permits, in addition to the requisite fiber network infrastructure.

As we come further, it is vital to comprehend that the OAN has two types of models, including two and three layers. In -the third layer OAN model, the physical layer—the fiber infrastructure is owned by one company or city municipality. A second company runs the operations, maintenance of the network, and provisioning of services, and the retail service providers provide the third layer.

In contrast to traditional municipal networks, where the municipality owns the network and has only one service provider, the open access model allows multiple service providers to compete over the same network at wholesale prices. It enables service providers to make money in the short term and the municipality to recoup its costs over the long period.

2.3. Essential role of private wireless networks in smart cities

The cities are transforming into digital and intelligent cities, focusing on the quality of life and improving the living standard, aiming for a sustainable or future-proof that is the vision of smart cities. Smart cities & municipalities are investing in technology to improve sustainability and efficiency to create a better future. The number of interconnecting devices is drastically growing, which requires reliable connectivity and high performance. These increases in devices in digital cities require massive real-time communication, security, high-speed connectivity, and low latency. The increasing of connected devices and excessive demands of constraints lead cities to adopt private wireless networks.

The capabilities of today's technologies like LTE and 5G that connect smart objects, people, and sensors using IoT devices can achieve the excessive demands of smart cities like massive real-time communication, security, and low latency. These technologies involve a radio access network and hybrid, or standalone models needed for deployment. The private deployment of these technologies, or what can be called a private wireless network, can achieve by using reserved spectrum frequency within a smart city environment. With these massive deployments of IoT devices, critical and massive communication is not easy to accomplish by traditional fiber optics deployment in smart cities due to many factors such as indoor and outdoor excessive coverage, fiber deployment time and cost, and intermediate devices. In contrast to the private wireless network, that is effortless deployment with incredible speed, fast adoption of technology, and responsiveness.

Efficient urban planning, while increasing the population daily in urban areas, requires effective initiatives to accelerate the smart cities' digital transformation efforts. Private wireless networks in smart cities must be endorsed to attain the smart city's critical success factors and struggles.

2.4. Private wireless usage benefits

Privately owning a wireless network means removing the dependency on providers. Exclusively owning a network allow cities to control operating models, networks not for the public and independent that permit management to apply their security policies and procedures for optimization. Network traffic is always inside the private network, bringing strong security within the network, specifically for mission-critical control for applications and equipment essential for the intelligent cities core network, such as used within the government, health, or financials. It also brings ultra-low latency and achieves extreme capacity or data rates, such as traffic monitoring and controlling an autonomous vehicle within the cities. In addition, one of the most significant benefits for the private wireless network is for massive IoT to achieve in-depth coverage – reaching challenging locations and ultra-high density to cover the massive deployment such as sensors or controllers. Managing IoT and video using a private wireless network can eliminate the cost associated with fiber deployment time, cost, and intermediate devices.

Usage benefits are as follow:

- Scalability
- Access and availability
- Cost reduction
- Network coverage
- Flexibility
- Network Security
- Increased efficiency

In a nutshell, private wireless networks in smart cities improve productivity toward digital cities and faster adoption of technologies that demand real-time computing. It also significantly improves quality, privacy & security as an independent, reduces operational expenses, and eliminates interruption.

3. Wireless network technologies, evaluation & benefits

Wireless network technologies are the approach to avoid the expensive implementation process of physical connection with a cable/fiber. It can be a connection within a facility or between various equipment sites. At the moment, wireless technologies are being implemented using radio spectrums that can be licensed or unlicensed.

3.1. Wireless network technologies

Different wireless network technologies include WPAN, WLAN, MANET, MAN, WAN, Cellular networks, and private LTE/5G networks.

WPAN: The WPAN is a wireless personal area network for the private reach network, such as the interconnectivity of Bluetooth radio and infrared.

WLAN: The WLAN is a wireless local area network, usually a point of internet access, a connection between devices over a short distance. Most WLANs follow the Institute of Electrical and Electronic Engineers (IEEE 802.11) standards denoted as WIFI. There is a point-to-point link used in fixed wireless technology implementation. Fixed wireless technology usually uses the microwave. But in some scenarios for fixed wireless networks, other technologies like satellites are used for the network connection between cities or buildings without any wire connection.
MANET: The MANET is a wireless mobile ad hoc network of radio nodes arranged in a mesh topology. Nodes work as forwarders to the subsequently available nodes, and nodes conduct routing.
MAN: The MAN is a wireless metropolitan area network that merges several wireless LANs. WiMAX is one type of MAN network.
WAN: The WAN is a wireless wide area network generally used for large areas like connecting cities. This network used to connect office networks between cities. The connection between two points is usually a point-to-point with microwave links. **Cellular networks**: A radio network consisting of cell sites, a fixed site working as a transceiver time known as a base station. Different radio frequencies in various cellular networks for the transmission and several kinds of frequencies in the transmission to avoid interference. The transmission among these cell sites provides radio coverage for that specific cellular network in a wide area.
Private LTE/5G networks: The LTE or 5G network is a wireless voice and data network used under licensed, unlicensed, or shared spectrum.

Table 1 Wireless Network Technologies

3.2. Wireless network evaluation

The idea of the wireless network or wireless technologies started in 1880 after the discovery of radio waves, leading to mobile phones or telegraphs. Later in 1922, FM frequencies were found along with portable radio. At that time, the framework was established for FM frequencies. In 1970, It was further supported, and the development of the internet and transmission came out that worked with high-speed packets.

The extraordinary evolution journey started in 1983, the first generation (1G), and it continues to reach wireless new generation 5G and even new technologies like LIFI. The G stands for generation, and each evaluation came out after research and development. There was a significant jump in this evaluation when 2G, the second generation, was released when wireless networks evaluation reached another era from analog to digital.

FIRST GENERATION (1G)

The first-generation standard was established in the 1980s and first introduced in Australia by the telecom company Telstra in 1987, which utilized a 1G analog system in a cellular mobile phone network. The 1G wireless network had poor voice quality and security with a maximum speed of 2.4 Kbps. The 1G analog system continued until the second generation, 2G, the first digital wireless standard.

SECOND GENERATION (2G)

In the 1990s, the second generation was introduced, and in 1991 the first commercial network was launched in Finland. The 2G primarily uses GSM standards and is new compared to 1G as 1G works using analog signals while the 2G network is the first digital network. The digital network comes with more security, reduced interruption, and safety with digital encryption. Furthermore, the network introduced multiplexing, allowing multiple users in a single channel and using circuit switching for data transmission.

The generation also presented a new way of communication that is still being used in many ways, such as

- SMS (Small messaging services).
- GPRS, The wireless technology introduced by 2.5G included GPRS (General Packet Radio Service) and presented multiple services, such as
- WAP (Wireless Application Protocol) access and
- MMS (Multimedia messaging services).
- EDGE (Enhanced Data rates for GSM Evolution) was introduced later in the same generation, 2.75; this technology is the extended version of GPRS, allowing precise and fast transmission up to 384 kbit/s.

  Also, it includes internet services like email, world wide web access. The GPRS provides a data rate range from 56 kbits/s to 115 kbits/s.

THIRD GENERATION (3G)

The 3G came up with a combination of a 2G network along with new technology and protocol to deliver a significantly faster data rate. Packet switching was introduced for data transmission in a 3G wireless network. The high-speed 3G wireless network was initiated in the 2000s with HSDPA (High-Speed Downlink Packet Access). Later in this generation, 3.5G and 3G+ or turbo 3G were introduced, which allows higher data transfer speeds and capacity on a network base on UMTS (Universal Mobile Telecommunication System) as its core network architecture. The 3G wireless network enables wireless communication, such as industrial and media streaming like radio and television transmissions.

HSDPA supported downlink speed up to 14Mbit/s in the early stage of 3G, and it increased to 42 Mbits/s of downlink with HSPA+ later in release 9 of 3GPP (3rd generation partnership project) standards. After that, the speed increased up to 84Mbits/s.
The 3G wireless network increased the efficiency of frequency spectrum utilization by utilizing the same frequency for multiple connections.

FOURTH GENERATION (4G)

The 4G extends the 3G wireless technology network with more services and bandwidth. The primary purpose of 4G is to increase the speed and provide high speed along with more security, capacity, and quality and lower the cost of communication usage. The purpose of the 4G introduction is the high-speed steaming over end-to-end internet protocol, and it comes with many functionalities and enables applications communication like mobile web access, video conferencing, IP telephony, 3D television, or cloud computing.
The two leading technologies on 4G as standards, commercially launched were,

- WiMAX (Worldwide Interoperability for Microwave Access) standards
- LTE (Long Term Evolution) standards, which ITU introduced in 2010.

It was first introduced and offered these standards in wireless communication in Scandinavia by TeliaSonera.

4G is the first entirely IP-based wireless network. All connections to the network are through the IP network.

Fifth Generation (5G)

Consumer demand is increasing, and communication standards are substantially changing to meet customer needs. The traffic and communication rise is anticipated to increase 10-100 times and grow before 2030. Connected devices are multiplying to fulfill the demands like application, transport, security, industrial, and home automation. For this purpose, intelligently connected cities and interconnected people require transporting enormous amounts of data in real-time that need high bandwidth, high security, and lower latency.

The projected estimation of connected devices can reach 50 billion in the next couple of years. 5G can support a high volume of data transmission, security, and lower latency but also works for remote advance medical service, virtual and augmented reality, and real-time communication like industrial automation. The legacy wireless networks generations 3G or 4G cannot compete and sustain these services.

The 5G technology overcomes many challenges, including.

- a massive increase in connected devices (IoT); there is a need for higher data rates, low latency, reliability, and security. The 5G brings all these together and adds value by reducing power consumption, which benefits the vast deployment of connected devices.
- In addition, 5G provides excellent reliability for emerging technologies such as in smart cities deployments, real-time data monitoring and controls, and virtual and Augmented reality.

To resolve issues related to the restricted frequency band due to the continuous deployment and operation of sophisticated technologies, the International Telecommunication Union (ITU) made specific standards to launch 5G in 2018. In these principles, to meet the 5G anticipations of large bandwidths, the 5G backhaul is allocated with millimeter frequency bands.

Hence, the noticeable boost in wireless devices came up with the problems of inadequate bandwidth and limited channels. Capacity has significantly lifted efforts to design and develop advanced next-generation standards for communication networks. Using the millimeter spectrum, 5G brings better channel capacity and higher data rates to meet the communications demand.

Smart cities are expanding with technological advancements. However, the more improvement in the applications and connected devices in the smart cities have less capacity, scaling is not vast, operations are slow, and some are not even possible with the technologies before 5G. To defeat all the mentioned challenges. The 5G is the key to success for all these initiatives that need advanced technologies, colossal capacity, scalability, low latency, and real-time advanced connectivity or operations.

<u>5G ARCHITECTURE</u> (5G Core)

Services split 5G network functions. due to this division, the 5G architecture is known as the 5G core Service-Based Architecture (SBA). The critical components are shown in the below diagram of 5G architecture that shows the 5G network topology.

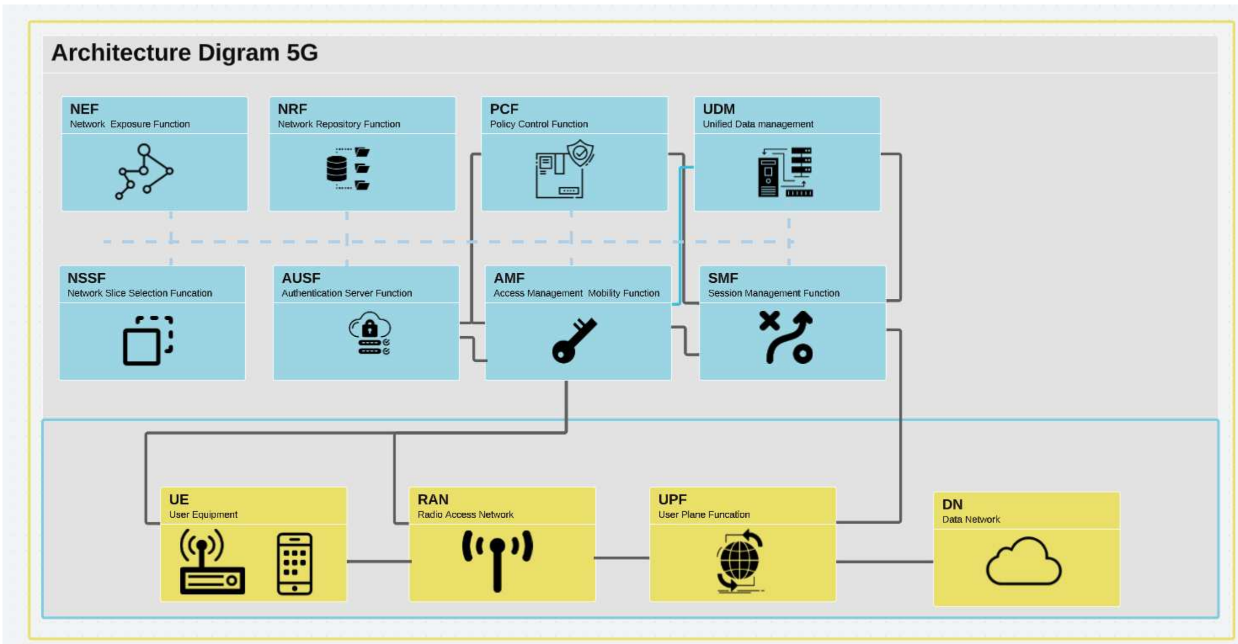

Figure 1 Architecture Diagram 5G

Explanation of critical components

UE: User Equipment such as end-user intelligent devices (5G smartphones) that will be further connected to the data network through 5G RAN.

AMF: Access and Mobility Management Function works as a single-entry point for UE connection.

SMF: Session Management Function, on establishing a service request by UE, the AMF function is to select the correct session management function and manage the UE session.

UPF: User Plane Function, the UPF is responsible for transporting the IP data traffic between the external network and UE.

AUSF: Authentication Server Function, AUSF allows Access and Mobility Management Function to authenticate the UE and 5G core access services.

The functions mentioned above work and provide the policy decision, session information, and policy control framework and also operate to control network behavior. It includes PCF (Policy Control Function), UDM (Unified Data Management), and SMF (Session Management Function).

<u>PUBLIC 5G VS PRIVATE 5G NETWORK</u>:

Both of the 5G networks, private and public, will offer dazzling speed, remarkably low latency, and network slicing.
Adopting a private 5G network will be a game-changer for enterprises, explicitly for businesses in which 5G competencies are required to accomplish the application transformation targets to propel.

- intelligent manufacturing
- digital transformation
- Internet of things (IoT)

IoT active connection is expected to be doubled in the next two to three years. The critical data for business and network access must be secure without an outage. Whereas, the public wireless network has limitations and security concerns for business-critical data that lead to private network usage.

PUBLIC 5G NETWORK	PRIVATE 5G NETWORK
Public 5G can be used by anyone through MNO. It can be any company or business. This may lead to an uncontrolled situation which can cause network congestion.	It can be used by only specific organizations that owned or licensed the private network. For this reason, it is more controlled by prioritizing and permitting various access levels.
For connectivity, Users need to be in a 5G network area, for example entire city	Private network is limited to a locality.
It is a shared network, maintained, deployed, and operated by a network provider	Enterprises don't share their network with other cellular networks in proximity. In the case of an independent 5G private network, the organization is responsible for its maintenance.

Table 2 Public vs Private 5G Network

Moreover, the increased enactment and efficiency of private 5G networks empower the user experience and achieve the innovative city vision.

The general sector and smart cities have a remarkable position in discovering 5G possibilities and leading the path around 5G principles, data privacy, values, and inclusivity.
In addition, 5G network slicing enables service providers to build virtual, end-to-end networks for fulling the requirements.

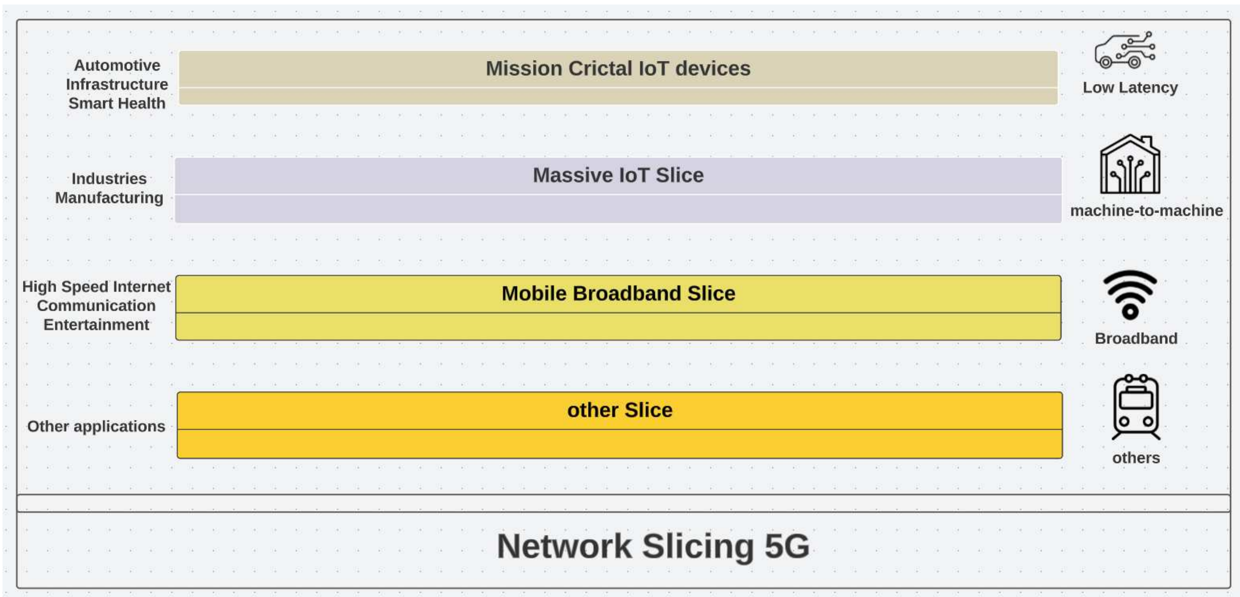

Figure 2 Network Slicing 5G

<u>Light Fidelity (Li-Fi)</u>:

LiFi is a new technology that uses light sources to transmit data.
A wireless communication system called Li-Fi (LiFi) uses light to transmit information and coordinates between devices.
The visible, ultraviolet, and infrared light spectrums can all be used by Li-Fi to transfer data at high speeds. Only LED lights can currently be used to transmit data in visible light.
Li-Fi is primarily used in military facilities, hospitals, and airplane compartments.
Li-Fi is a variation of optical wireless communications (OWC) technology, which works similarly to Wi-Fi in that it uses light from light-emitting diodes (LEDs) as a medium to offer network, mobile, and high-speed communication. With rates of up to 224 GB per second, it transfers data using regular LED light bulbs in homes.

The 3GPP defines three primary 5G use cases as part of its SMARTER (Study on New Services and Markets Technology Enablers) project. The purpose behind the SMARTER project was to design & develop high-level use cases and determine what segments and functionality 5G would require delivering to facilitate them. It was initially grouped into five classifications when it started in 2015 with 70 use cases, which were grouped again into three categories. “Massive IoT,” “Mission Critical-Control,” and “Enhanced Mobile broadband.”

3.3. Massive IoT

In the 5G world, vantage has been propelled towards a higher level. As we approach a future with millions of connected devices per square kilometer, plenty of those require high bandwidth connectivity. The Massive Internet of Things is used for deep coverage to reach challenging locations, ultra-low complexity, such as where 10 bits per second is required, and for ultra-high density, where up to one million nodes per kilometer square (KM2) is needed. The application that involves low cost and low energy defines many endpoints that may continuously serve small bits of data, mostly to distant locations— a huge amount of data that needs to be delivered on a regular basis to the endpoint or cloud. IoT sensors from various machines, objects, and devices can communicate with each other and collect data for analytics that are efficacious for improvement and decisions in real-time. IoT sensors require versatility and scalability; these devices generally utilize less power and moderate cost. Furthermore, it needs adequate capacity for massive IoT, security, and network efficiency to communicate with millions of devices. All these challenges are attainable with 5G.

5G connectivity and LPWAN (Low Power Wide Area Networks) are vital components for adopting IoT solutions and connecting millions of devices. It comprises both licensed and unlicensed frequencies. It supports and covers all these Massive IoT applications and devices challenges. Examples of massive IoT are.

- smart buildings
- smart metering
- intelligent traffic monitoring or traffic controlling/ rerouting
- smart irrigation
- industrial IoT
- smart homes

These use cases were and are supported by 4G but with numerous shortcomings. Having 5G, we can cover these challenges and multiple use cases where reliability, scalability, network efficiency, and capacity is demand.

3.4. Mission-critical control

Mission-critical control is used where fewer endpoints involve with enormous levels of data. Massive critical control incorporates strong security, such as for innovative health care, government, or financial sector; it provides ultra-high reliability where a rate requires less than 5-10 per one millisecond. It also includes ultra-low latency, requiring less than one millisecond. It is described as URLLC (Ultra Reliable Low Latency Communications). It involves more complex scenarios with high bandwidth and ultra-low latency in addition to just data collection. The complexity and high demand of different factors in mission-critical control become a reality with 5G initiation; merely 5G can overcome these challenges and accomplish the request for upgraded requirements.

Critical IoT can meet the demand for new processes in manufacturing industries; it can support the broad scale network with scalabilities, such as controllers, machine-to-machine, and robots. In addition to ultra-security and protection, end-to-end communication between devices, such as threats and network attacks. The applications in mission-critical control include virtual reality (VR), robotics technologies, smart hospitals such as remote surgeries, or intelligent industrial control by machines with data decision models or traffic control and safety. All these applications call for massive data for communication in real-time, and minor loss could lead to the failure of the operations. These all require ultra-low latency along with time-sensitive information, and failure or loss of communication, data transmission, and missing data can lead to system failure. So, these systems demand critical factors that need deep designing of the system and communication between devices to overcome the challenges of mission-critical control use cases.

3.5. Enhanced mobile broadband.

The enhanced Mobile broadband (eMBB) is the first 5G service and extension of the 4G services. Ericsson estimates that by 2023, 5G subscribers will reach one billion globally. At the start of 2017, the 3GPP initially committed to finalizing the non-standalone (NSA) 5G, and the first standard was approved in December 2017. The initial prototype aimed to use the 4G network with 5G to reduce latency and boost the data rate. In 2018, the standalone 3GPP 5G core network architecture standard was completed. Multiple releases by 3GPP started in 2018 with release 15 and a use case of vehicle-to-x service. First, it introduced real-time traffic alerts, streaming real-time videos that involve 3D and high-speed internet, followed by autonomous vehicles that are vehicle-to-vehicle communication and interact with surrounding road infrastructure.

The enhanced Mobile broadband (eMBB) is a natural transition from 4G networks that can provide a better user experience and faster data rates. In addition, it enabled 360° video streaming and introduced AR & VR technologies along with many others. Furthermore, the 5G main attribute was set to deliver higher capacity, enhanced connectivity, and higher user mobility.

3. Open and licensed spectrum

Radiocommunication devices operate with the spectrum, either licensed or unlicensed. The radio frequency required for all wireless communication necessitates massive planning as the radio frequency can reach a cross border that can interfere with each other while using the same frequency. In today's modern world, we are rapidly shifting to transform ourselves to innovative technologies, and most are interlinked, stipulating the allocation of radio frequency. The utilization of radio frequency and interference requires some regulations and control. The radio frequency spectrum is regulated and legally bound by intergovernmental under ITU (International Telecommunication Union). The international spectrum planning, standards, regulations, policies, enforcement, interfaces disputes, and allocation of the different frequency spectrums are incorporated in meetings between all countries, each after a couple of years in WRC (World Radio communication Conferences) held by ITU. In addition to all nations, it includes the world's public and private sectors to support and explore the impact of fast-moving digital technologies that help radio regulations incorporate the final acts of WRC between all nations to agree on binding resolutions and non-binding recommendations.
The flourishing demand for advancement, increasing the number of connected devices, the rapid evolution of digital technologies, and the growing development of IoT and technology like 5G require a broader frequency band range. This magnifying consumption of the radio frequency spectrum and high demand requires efficient planning to control or allocate spectrum and to ration its uses, forcing users to be well-organized by giving priorities to invest in efficiency improvements on utilization.

An increase in devices in digital cities requires massive real-time communication, which proliferates and increases the competition of a limited capacity spectrum. One way to increase the capacity is to build more base stations for the deeper network, which will multiply environmental issues. The utilization of the spectrum involves efficient planning to use the spectrum, such as dynamic sharing of the spectrum or other ways to improve the utilization.

The spectrum requirement depends on individual use cases, such as some industrial automation requiring more latency and environmental sensors demanding fewer restrictions.

On the other side, smart cities seek high capacity and low latency connectivity because of the use of automated vehicles or a considerable number of IoT-connected devices & their communication.

The radio spectrum has different bands and uses for various radio communication. The radio spectrum is divided into licensed and unlicensed channels. Licensed are controlled and assigned by governmental bodies to exclusive operators, while unlicenced are held for standards and regulations but open for public use.
In the United States, FCC, which is a federal communication commission, manages and controls spectrum frequencies. FCC set principles, including licensing to operators.

4.1. Licensed Spectrum

The licensed spectrum has its advantages over the unlicensed as licensed spectrum for wireless communication has vital parameters that are

- no congestion
- least interference

Furthermore, the license frequency spectrum has more acceptable technical performance because of its significant benefits, enhanced reliability, improved performance, and less noise.

We have more advantages on the licensed frequency spectrum, so it is more secure for operators or private companies. Many smart cities and municipalities are moving forward to secure the network and communication and working on having their private wireless network. It is the desire by many private own companies/municipalities cities or even government owing projects to have their frequency spectrum. A considerable disadvantage of the frequency spectrum is the limitation, license, and equipment cost associated with having a private spectrum.

4.2. Unlicensed Spectrum

The unlicensed spectrum is regulated but open to public use without cost. Most Wi-Fi operators in the open public are licensed. Unlicensed spectrum band equipment is extensively accessible at reasonable. In addition, it provides flexible cellular network deployment for MNO (Mobile Network Operators) for interference administration.

Due to performance issues, MNO (Mobile Network Operators) or ISP typically do not use unlicensed or unrestricted frequency spectrums. There are further issues of interference and congestion with the unlicensed frequency spectrum.

4.3. Smart City wireless Spectrum

Smart cities are reshaping the life experience, and new developments in contemporary infrastructure represent a completely different approach to technology modifications. Connecting millions of devices and sensors, then handling the generated data, smart cities must establish ultra-reliable connections, robust, low latency, and real-time communication. Achieving extreme capacity or data rates along with high-speed wireless networks is challenging for city planners and designers.

Implementing these advancements and connecting people with interconnected cities that will enhance the way of living, such as improving public safety and reducing traffic congestion, are the central pillar of smart cities. These evolutions in smart cities make the future achievable with wireless spectrum.

IoT devices play a crucial role in advancing frequency allocation in smart cities. In most municipalities and smart cities, an unlicenced frequency spectrum is used. Transmission dedicated licensed frequency spectrum is considered to avoid degradation and boost performance in IoT.

4.4. 5G Spectrum

3GPP defines two sets of frequency spectrum based on.

- MIMO (multiple input, multiple outputs)
- antenna system
- spatial multiplexing, or space-division

The 5G frequency spectrum is classified into two frequencies.

- FR-1
- FR-2

<u>FR-1 Frequency Range</u>

FR-1 Frequency Range is used for most traditional cellular mobile communication, ranging from 4.1GHz to 7.125 GHz. It is also called a low-frequency band, namely sub-6 GHz.

FR-2 Frequency Range

FR-2 frequency range is capable of high data rate and focused on short range. It ranges from 24.25 GHz to 52.6 GHz. Its high-frequency bands are often referred to as mmWave (Millimeter wave).

Transforming to 5G from such as LTE is the primary goal, and it is not possible in one move; sharing of the spectrum is commonly used in TDD (Time-division duplexing) and FDD (Frequency Division Duplexing) usage. Due to many limitations during this transformation, all three significant types of use-case of 5G (eMBB, uRLLC, and mMTC) still need to be implemented. However, many use cases have been implemented with licensed spectrum, such as in the United States, Canada, and Europe.

Selection and Usage of Low Frequency and High Frequency:

Table 3 Frequency

FR-1 Frequency:	FR-2 Frequency:
● FR-1 Frequency Range is low frequency, called sub-6 GHz. ● FR-1 frequency is the primary band for 5G. ● FR-1 sub-6 GHz is the best fit where the low frequency is required, such as for long-distance propagation. ● FR-1 sub-6 GHz is the best fit where the low frequency is required, such as for long-distance propagation.	● FR-2 Frequency Range is high frequency. Its high-frequency bands are often referred to as mmWave. ● These are the extended bands for 5G. ● In the use-case of low latency, such as live streaming, the 5G mmWave is suitable and fulfills the need at the enterprise level where the area is dense, but the coverage required is bounded to specific premises. The use of mmWave is the best fit for these use cases.

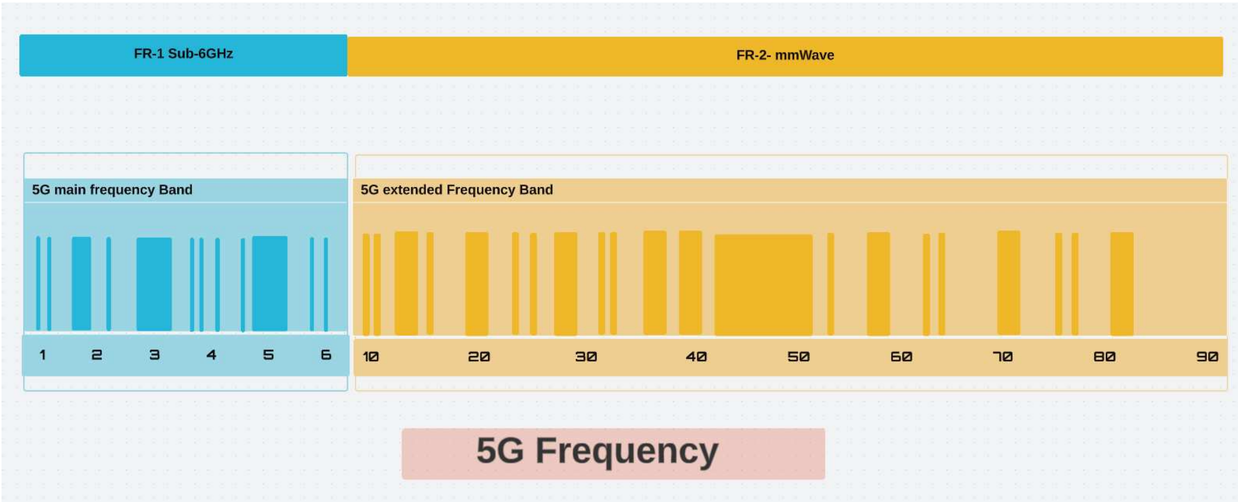

Figure 3 5G Frequency

5. Challenges & issues of the private wireless networks in smart cities

Smart cities are practicing the latest 5G and IoT technologies to provide digital solutions and improved living standards.5G has already started playing a crucial role in the tremendous development of smart cities and the innovation of technologies. There is still a long way to accomplishing and delivering the promised milestones of 5G, such as the Massive Internet of Things (M-IoT), security, and public safety for advanced applications.

In recent years, companies and mobile operators have been consistently working and focused on developing the groundwork to be in operation for the 5G. Now, the framework is built, and 5G is in the next phase of implementation and utilizing its capabilities that enable many advancements to move into reality.

Wireless network, specifically 5G, is still in the early stage of implementation, adoption, along with development as well. So full function and capacity of 5G need to be analyzed in detail, and many improvements still need to be developed and adopted for the 5G wireless network. The early adopters need to evaluate benefits along with challenges toward success.
The significant impacts of adopting 5G wireless are:

- capacity
- higher bandwidth
- high speed
- low latency
- reduced interference and communication delays.
- greater coverage

Cities are deploying connected devices such as intelligent traffic lights, smart traffic monitoring and controlling, smart parking, smart metering, and sensors that enable them to be connected and make them smart cities. The vast number of devices and interconnected sensors on other infrastructures for instance low-power machines communication, or intelligent homes where several end users are using the data from these sensors and interacting with the controls and data for decisions. Each new connecting device sums up the number of entry points into the network. It leads to cyber security issues. With the tremendous data or connectivity of high-density systems and innovative technologies in smart cities, only 5G wireless can cover the high bandwidth and capacity to overcome and fulfill the current and future demands. 5G framework can meet today's challenges.

The considerable amount of data from different interconnected devices and sensors can support progressive technologies for accurate insights and the ability for further decisions and management of cities. The capabilities of 5G bring and deliver substantial connectivity to enable the deployment of millions of devices and analyze the data in different aspects. Such as crowd management, security management, traffic management with traffic data, automation of traffic flows or rerouting the traffic or waste management, or smart energy that is only possible with data analysis in real-time and 5G is able to address these challenges. Technologies we have, or next-generation technologies, will surely need effective deployment that needs interconnected wireless infrastructure for the smart cities, 5G enables all these real-time connectivity challenges.

Along with the benefits of this wireless invention, several concerns need to be addressed, and companies are working to improve it. There are many problems with enabling new technologies or interconnectivity wireless networks.

Increase in interconnected devices:

In modern times, we consider the 5G technologies to fulfill the requirements of smart cities. Their capacities, such as high bandwidth or low latency, give us more devices and connectivity. Moreover, these new layers of extensive linking of millions of devices need more network points to connect; these end points toward the network also bring cybersecurity liability.

These security issues need to be taken care of appropriately. It can be a substantial risk as several industries connect equipment and sensors, escalating more significant cybersecurity attacks. To manage these threats, suitable design and management of interconnectivity are essential for wireless networks. For this purpose, 5G is considered to have enhanced security capabilities. These attacks can vary from minimal human error to critical cyber threats. Daily, a vast amount of sensitive data is channeled through a network with cyber vulnerabilities. Therefore, a private network is becoming a fundamental need for our future. Smart cities are practicing the latest 5G and IoT technologies to provide digital solutions and improved living standards.5G has already played a crucial role in the tremendous development of smart cities and the innovation of technologies. There is still a long way to accomplishing and delivering the promised milestones of 5G, such as the Massive Internet of Things (M-IoT), security, and public safety for advanced applications.

In recent years, companies and mobile operators have been consistently working and focused on developing the groundwork to be in operation for the 5G. Now, the framework is built, and 5G is in the next phase of implementation and utilizing its capabilities, enabling many advancements to move into reality.

Wireless network, specifically 5G, is still in the early implementation, adoption, and development stage. So full function and capacity of 5G need to be analyzed in detail, and many improvements still need to be developed and adopted for the 5G wireless network. The early adopters need to evaluate benefits along with challenges toward success.
The significant impacts of adopting 5G wireless are:

- capacity
- higher bandwidth
- high speed
- low latency
- reduced interference and communication delays.
- greater coverage

Cities are deploying connected devices such as intelligent traffic lights, smart traffic monitoring and controlling, smart parking, smart metering, and sensors that enable them to be connected and make them smart cities. The vast number of devices and interconnected sensors on other infrastructures, for instance, low-power machines communication, or intelligent homes where several end users use the data from these sensors and interact with the controls and data for decisions. Each new connecting device sums up the number of entry points into the network. It leads to cyber security issues. With the tremendous data or connectivity of high-density systems and innovative technologies in smart cities, only 5G wireless can cover the high bandwidth and capacity to overcome and fulfill the current and future demands. 5G framework can meet today's challenges.

The considerable amount of data from different interconnected devices and sensors can support progressive technologies for accurate insights and the ability for further decisions and management of cities. The capabilities of 5G bring and deliver substantial connectivity to enable the deployment of millions of devices and analyze the data in different aspects. Such as crowd management, security management, traffic management with traffic data, automation of traffic flows or rerouting the traffic or waste management, or smart energy that is only possible with data analyses in real-time and 5G able to address these challenges. Technologies we have, or next-generation technologies, will surely need effective deployment that needs interconnected wireless infrastructure for the smart cities, and 5G enables all these real-time connectivity challenges.

Along with the benefits of this wireless invention, several concerns need to be addressed, and companies are working to improve it. There are many problems with enabling new technologies or interconnectivity wireless networks.

<u>Increase in interconnected devices</u>:

In modern times, We consider the 5G technologies to fulfill the requirements of smart cities. Their capacities, such as high bandwidth or low latency, give us more devices and connectivity. Moreover, these new layers of extensive linking of millions of devices need more network points to connect; these end points toward the network also bring cybersecurity liability.

These security issues need to be taken care of appropriately. It can be a substantial risk as several industries connect equipment and sensors, escalating more significant cybersecurity attacks. To manage these threats, suitable design and management of interconnectivity are essential for wireless networks. For this purpose, 5G is considered to have enhanced security capabilities. These attacks can vary from a minimal human error to critical cyber threats. Daily, a vast amount of sensitive data is channeled through a network with cyber vulnerabilities. Therefore, a private network is becoming a fundamental need for our future.

<u>Regulations issues</u>:

Extensive deployment and broad-ranging wireless networks like 5G implementation for intelligent cities require legitimate regulations. These regulations allow different towns, providers, and consumers to have adequate service level agreements for connected devices, such as roaming nationwide or internationally or rules that enable various providers and integrators to work together to deliver and operate the network for interconnectivity.

<u>Monetization with multiple stakeholders</u>:

The deployment & implementation of these new technologies in tremendous amounts also lead to liability regarding any problem that might arise. In 5G, multiple stakeholders, such as integrators, operators, business partners, internet service providers, network vendors, platform vendors, device manufacturers, and application providers, must work together to achieve the immense formation of interconnectivity. Monetization also needs to be appropriately defined for most use cases for smart cities; different stakeholders' involvement is complex as the business partnership. In addition, it generally requires high-cost CAPEX and OPEX. Therefore, it is considering the implementation of the wireless network (5G) that provides an ideal technical framework for wireless connectivity and long-term benefits.

Furthermore, it needs to manage the CAPEX and OPEX in the long term with different stakeholder and cost models that is commercially viable. Therefore, the flexible business and cost model that needs to be adopted is the key to success with these advancements in vast development.

6. Security concern on IoT network with 5G private wireless network

With the rapid transformation of digital technology advancements, particularly in wireless networks with 5G and IoT deployments, multiple cybersecurity issues are primary concerns. The critical ones are data exposure carried on the wireless network of connected devices, attacks on network equipment and devices connected to the network, and data privacy and compliance requirements.

Numerous challenges exist in deploying 5G. Gradually, Security has been improved, and new technologies have been realized. Though it needs to be followed, more betterment may need to cover all future expected difficulties.

Compared to other wireless network technology like 4G, 5G has more capacity and it can attain many use cases that were unfeasible in the past with other generations. Moreover, the 5G wireless network has advanced new features and services covering security concerns. Some are as follows.

- Enhanced capabilities with 5G New Radio (NR).
- spectrum sharing & increased the spectrum.
- Bandwidth frequencies include low, mid, and high.
- Reduce interfaces, Cell densification to serve vast numbers of users.
- Multi-access Edge Computing (MEC) introduced in 5G improve customer experience. It increases the data transfer rate with a high data volume and reduces the latency. Smart applications run and deliver over 5G, and with MEC, it centralizes applications and is closer to the edge to reduce the latency.
- Introduced network slicing, that is, multiple virtual networks providing different types of quality of service using the same physical network infrastructure.

3GPP has also addressed security issues and 5G wireless network improvements. From the first phase of mobile standards in the 1980s, 3GPP has played a significant role in the generational advancement that occurs roughly once per decade. The system has improved with each generation, as measured by 3GPP Releases. It has incorporated more reliable encryption algorithms. Security has made many improvements, some of which are noted below.

5G Security Improvements (Standalone Architecture)

Subscriber Security and Privacy Encryption of unique device identifiers to mitigate rogue base stations. Mutual authentication of subscriber and network. Confidentiality and integrity protection for control (signalling) traffic and user (data) traffic. Ability to restrict radio technologies that a device uses (e.g., turn off 2G/3G).	RAN Security and Privacy Use of a massive number of antennas and beamforming techniques to reduce interference and make it harder to conduct over-the-air eavesdropping attacks. RAN is separated into distributed units (DUs) and centralized units (Cus), with Dus located near the antenna and Cus, which store sensitive information, placed inside a trusted and physically secure location.
Core Network Security Shift to service-based architecture with Transport Layer Security-based authentication and encryption. Options for Internet Protocol Security and attribute-based security across each interface. Service-based discovery and registration to support confidentiality, integrity, and replay protection.	Roaming Security Security gateway for roaming interconnects to enforce control plane security policies. A home network can verify if a device is present in the serving network when it receives a service request from the serving network. Protection of user plane traffic between two networks.
Network Slicing and Virtualization Network slicing allows the isolation of data plane traffic as well as different security attributes for various user classes. Software-defined, virtualized network functions allow for rapid reconfiguration to respond to attacks.	Authentication Subscriber authentication is completed by home network (helps protect against false base station attacks). Authentication is open and agnostic to the RAN. 3GPP and non-3GPP access networks (e.g., Wi-Fi) use the same authentication procedures.

Table 4 Cybersecurity Infrastructure

Reference Source: Cybersecurity and Infrastructure Security Agency (CISA) cisa.gov

There are numerous security enhancements with 5G. Additionally, leveraging private networks, such as wireless networks in smart cities that use 5G networks, strengthens the security perimeters. Because private networks are not shared with others, they operate more securely than conventional networks.

The complexity of corporate security cannot be validated for any enterprise by using it privately, such as in smart cities. Moreover, the wireless network of 5G is also sophisticated, which makes it challenging to define network security boundaries. These features include network uniqueness, huge machine-type communication, ultra-reliable and low-latency communication, and many others.

The Cybersecurity and Infrastructure Security Agency (CISA) has identified the following security threat categories. The same risks are associated with deploying 5G IoT in smart cities.

- Network and Management Interface Threats
- Application and Service Threats
- Privacy Threats
- Environmental and Physical Threats
- Artificial Intelligence/Machine Language (AI/ML) Threats
- Virtualization Threats
- General Cybersecurity Threats

7. Design considerations for private wireless networks.

Going on to new developments, considering the Internet of Things and linked devices, and more specifically private wireless networks like smart cities, 5G private wireless network enabled improved connection that was probably not achievable with earlier technologies. The 5G is intricate and constantly changing. Authorities must consider approaches for revision in standards, features, security threats, and policies in the growing wireless 5G network.

Design consideration of private 5G wireless network:

System model: Concerning 5G private wireless network, many factors need to be included, such as 5G Radio Access Network (5G RAN), Network Slicing, Multi-Access Edge Computing (MEC), 5G Core Network, and User Equipment on UNI (User Network Interface) & NNI (Network to Network Interface).

The 5G private wireless network design will likely incorporate multiple service providers, such as Cloud services to the network and 5G core provided by a service provider. In contrast, the application service provider MEC can be multiple and come from different providers, or any communication between NNI to UNI can be with various providers. Thus, it can be viewed as one system configuration with a collection of subsystems. Moreover, multiple owners may possess these subsystems. Therefore, the 5G private wireless network is more complicated and presents a greater security risk because it comprises various service providers.

The multiple possibilities for implementing the 5G private wireless network create a unique system with different attributes toward the design model.

Multi-Access Edge Computing (MEC): It aids in service provision and communication facilitation where extremely low latency is required. In addition, MEC boosts the end user's computational power. It can be a public edge cloud, MEC, or private MEC for a private network, such as in smart cities where some communication must be entirely private.

Radio Access Network (RAN): RAN connects UEs to private wireless networks. A 5G private wireless network can have a virtual, cloud, or open RAN and can include a variety of design models with varying ownership, security, and virtualization choices.

Core Network: In the 5G private wireless network, the core network authenticates subscribers, securing the connections and connectivity across numerous networks, and enabling communication with the NNI (Network to network interface). 5G private wireless core network provides access to services and secure transmission for several interfaces.

1. Transformation from a traditional network to a private wireless network

Over conventional wireless networks, a 5G private wireless network is intended to offer increased capacity, reduced latency, and security. However, the strategic deployment of devices in the network, the access, and the core network to implement the private wireless network, along with many other factors that make it more challenging to define the boundaries of the approach, contribute to the high complexity of a 5G private wireless network.

Transforming traditional wireless networks to private networks like 5G depends on the use case scenario. Developing the user equipment, Core network, radio access network, systems, and applications will typically be part of the transition to the new private wireless network. The private wireless network's usage, design, and implementation might alter according to the use case, such as enormous critical or low latency communication. The private wireless network can be built and executed with various configurations according to the particular situation. For instance, the private wireless network can be designed and operated as a completely standalone solution in intelligent cities. Alternatively, it can be shared or unlicensed spectrum usage in the town or municipality if it is not critical; it can also be licensed spectrum access. In some use cases, the government controls the infrastructure, owns the municipality or city, and acts as both the operator and owner of the property. It may also be privately owned by a business and deployed. Lastly, the design and execution might be hybrid or standalone, with different owners accessing the spectrum, infrastructure, operations, and applications.

To cover the same region, private wireless needs considerably fewer access points than traditional wireless options, which means less supporting infrastructure such as power, cabling, poles, etc. The attributes of the radio spectrum make designing and planning radio coverage substantially less expensive. Consequently, you can integrate your modern networks onto a single 4.9G/LTE or 5G network for significant operational cost reductions.

A private wireless network must be implemented to meet the high-speed and low-latency demands. Yet aside from lacking range, power, frequency, and capacity, the typical wireless network also needs to be improved.

Network Infrastructure: The transformation toward the 5G wireless network comprises network infrastructure where a private wireless network can be a subdomain of the network operators. In addition to operating, maintaining, and delivering the subnetwork/network slice to private wireless networks, such as those in smart cities or municipalities, the network operator also owns the public radio access and core network.

Spectrum: The spectrum in the private wireless network depends on the use-case scenario. For instance, the utilization of the range can be shared in cases when security and resilience are essential but not at the expense of the high-end. On the other hand, the licenced spectrum of a network operator is necessary for use cases that are security, real-time-or mission-critical. To reduce the cost of spectrum licencing and operation, the spectrum may be held by or under the network operator's control.

Security: Due to diverse use case situations, the security compliance criteria can be extended based on the use case. 3GPP defines the security features and measures in the 5G wireless network. Further security may necessitate improved protection and 3GPP-defined security procedures and features, such as network operators sharing spectrum with end-to-end security. Nonetheless, municipal or government criteria must still be met, and additional security measures must be undertaken. According to local government norms and regulations, IoT devices need extra security precautions, influencing the infrastructure or devices that need to connect.

2. Use Cases

Private wireless network use cases in smart cities are planned, designed, and deployed by performance parameters. Some use cases are feasible and functional with existing radio access networks using 4G or non-standalone 5G. Conversely, some can be accomplished by utilizing a virtual, private 5G network, which might necessitate network slicing. Moreover, some situations require a dedicated standalone private 5G network due to performance and robustness. In conclusion, deploying a private wireless network in smart cities can be accomplished with or without slicing; in other words, it can be a dedicated private 5G network, a virtual, or a hybrid network.

To support a wide range of use case requirements across numerous vertical initiatives in smart cities, including health care, traffic management, energy, public transportation, AR & VR, and numerous other sophisticated facilities, wireless networks implementing 5G are needed. Even with specialized private wireless networks, network slicing is frequently employed to target distinct projects or industries. Therefore, customization that supports different access network objectives, use cases, or business models makes sense. A use case's features are abstracted to determine the various types of network slicing. The Massive Internet of Things (mIoT), Enhanced Mobile Broadband (eMBB), Ultra-Reliable and Low Latency Communication (uRLLC), and Vehicle-to-Everything (V2X) communication are the four network slicing types that the 3GPP established to support 5G wireless networks.

Different slicing presents technological challenges and performance conditions, including power efficiency, spectrum efficiency, robustness, high reliability, lower cost, high energy performance, and low latency.

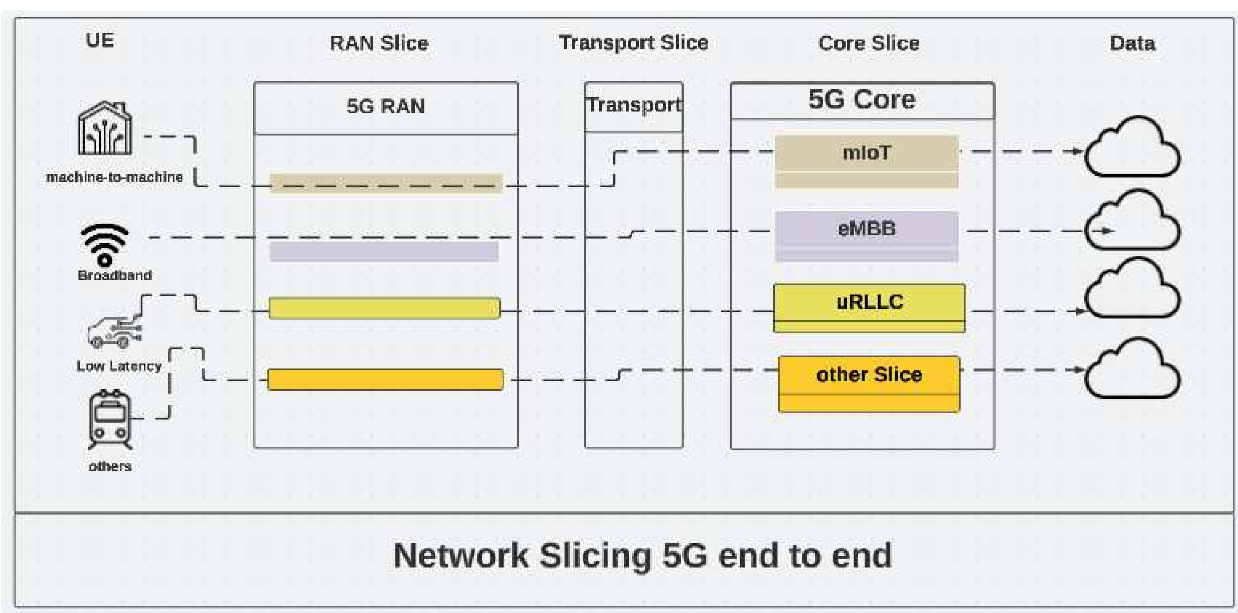

Figure 4 Network Slicing 5G end to end

9.1 Traffic management with IoT

Traffic management use case:

The automotive industry is proliferating, and an intelligent traffic management system is likely to be a must-have in many cities to control and manage traffic and control it for safety, reroute it for time savings, and provide road assistance Cities are therefore striving towards automated and intelligent transportation systems. Autonomous & connected vehicles are also growing in addition to overall automobiles. The projection of connected cars by 2025 is expected to be 400 million, while 54.2 million is projected for autonomous vehicles. Although the number of automobile consumers is increasing and even switching toward electric, connected, and autonomous vehicles, on the other side, the advancement and new technologies are embedded, such as advanced driver assistance systems (ADAS), projected to increase to 58.59 billion by 2028, automotive software or automotive cybersecurity systems that eventually need real-time monitoring, traffic management, road safety and traffic efficiency services, Intelligent navigation on the road.

With the rise of connected and autonomous vehicles, the necessity for intelligent transportation systems or traffic management has arisen. 5G is the enabler for many efforts in the automotive and traffic management industries.

Congestion in Smart Cities:

Increased automotive technology contributes to several issues across cities, including collisions, traffic congestion, pollution, automotive cybersecurity, and monitoring. However, as cities develop, municipalities have distinct issues with regard to services and infrastructure because of the steadily growing populations. Increased traffic that leads road congestion is one of the obvious effects of population growth. Traffic congestion increases the number of environmental, economic, and human costs such as time), fuel, vehicle maintenance, safety (such as emergency response time), crashes, supply chain and shipping delays, access to jobs, and environmental concerns, (such as the impact on CO2, air pollution, affect productivity and quality of life).

The future lies in advanced IoT solutions that can gather data to optimize services and infrastructure. These Internet of Things (IoT) devices, for instance, can gather data on different traffic patterns, volumes, and real-time traffic to monitor and regulate traffic by modifying traffic lights or rerouting through advanced signage based on traffic volume on a particular road. Furthermore, reducing congestion by enabling real-time parking availability becomes an intelligent parking system or wise emergency response time that can be achieved with real-time data from cameras and sensors that can assist the first emergency responder in analyzing video, audio or vehicle location that support trigger emergency responses.

Fast data rates, improved user experiences, mobility, strong connection support, and high data collecting rates per square kilometre are necessary. Massive IoT (mIoT) is a kind of IoT that supports numerous connected devices in a condensed zone. Also, the enhanced mobile broadband (eMBB) is designed to provide improved coverage and higher data throughput. With advancements in communication for gathering vast data, analyzing, optimizing, and applying AI through private wireless networks using 5G, increased data rate, coverage, and many linked devices can be achieved.

Intelligent Transport Systems have reduced accidents and traffic congestion in many municipalities and cities. However, these services and applications must enable the use cases for traffic management only achievable with 5G and the following constraints.

5G and traffic management constraints

- massive volumes of continuous data
- real-time data processing and delivering judgment & conclusion support.
- communication with low-latency and reliable networks

Issues:

Lack of traffic projection:(due to massive volumes of continuous data)
Commonly traffic light systems are implemented in a specified time slot. The static traffic control system does not depend on real-time traffic flow. Therefore, it is unable to anticipate or adjust according to the current traffic flow of the vehicles on the road. An intelligent traffic control system that can forecast based on significant traffic flow factors can reduce waiting time, decrease fuel consumption, reduce vehicle pollutants, and reduce the cause of climate change.

Lack of real-time traffic situation: (due to real-time data processing)
Commonly used traffic management systems have limitations that reduce effectiveness, such as lack of communication and traffic conditions brought on by real-time data and traffic flow. However, traffic in metropolitan areas can be significantly improved by factors like positioning, weather, vehicle speed, and traffic flow. High-resolution sensors and traffic infrastructure can be used to implement these, assisting in detecting traffic conditions and supporting intelligent traffic management systems like traffic rerouting, real-time information on the roadside, traffic lights, and quick responses to accidents and emergencies.

Lack of ultra-low latency connectivity & communication challenges:

Due to bandwidth constraints, the traffic infrastructure's growing linked equipment, communication, and data processing from sensors and high-definition cameras in the traffic management system is constrained. Therefore, real-time data collection for traffic management for further analyses and actions is challenging. In urban traffic management systems, low-latency communication is a must to benefit from large-scale real-time data for efficient usage. Lack of ultra-low latency, communication patterns such as dependent action from traffic data to monitor and efficiently control, or automated action are limited, and some are nearly impossible.

Traffic optimization approaches:

Several strategies for enhancing and optimizing traffic management systems have been adopted in the past. As a result, the traffic management techniques listed below are frequently utilized to improve and address traffic management issues.

- ATSC: Adaptive Traffic Signal Control
- V2X: Vehicle to anything
- VFC: Vehicular Fog Computing
- SDN Architecture: Software-Defined Networking based Architecture.

ATSC: Adaptive Traffic Signal Control:

The ATSC approach has been used for many last years with changes in the algorithms in the approaches. This approach uses traffic junctions, changing the traffic light schedule depending on the traffic flow instead of a fixed timetable for the traffic light. It supports traffic congestion.

V2X Vehicle to anything:

V2X, often known as vehicle to everything or vehicle to anything, is a networked transportation infrastructure. Radio communication is required for this linked transportation system infrastructure, necessitating real-time communication between the vehicle and its surroundings. It is the exchange of information between moving cars and other entities like traffic signals, other moving vehicles, pedestrians, the environment, and other connected equipment. The development of V2X technology is closely related to the expansion of interconnectivity. As a result, cities and infrastructure around the globe will be impacted. Furthermore, it will be intended to assist smart cities while minimizing traffic accidents, making roads safer, boosting traffic efficiency, and enhancing emergency response on the side of the road.

Freight road safety-V2X communication- work zone warning/weather warning and assistance to a driver:

Intelligent transportation system (ITS) solutions obtain real-time weather information, work zone information, and wind information from environment sensors stations or other measuring devices. For example, a driver's vehicle device will display real-time suggestions and warnings from ITS after processing information from the central hub.

VFC: Vehicular Fog Computing:

Fog computing, often known as fogging, is a cloud computing strategy where data extend from the center location to edge networks, making data accessible from the closest location. The fusion of vehicle data with fog computing is known as vehicular fog computing. This approach uses an edge point that immediately facilitates data interchange between vehicles to connect vehicular data to the cloud. It manages enormous data volumes and supports the secure, real-time interchange of sensitive information between moving vehicles and traffic management systems.

SDN Architecture: Software-Defined Networking based Architecture:

SDN aims to support traffic congestion while managing a large amount of data. Traffic management employs SDN architecture to address the transmission latency between vehicle communications and connectivity loss between infrastructure, such as controllers and traffic management systems. It aids in creating the optimal route and easing traffic congestion.

Limitation of Traffic optimization approaches:

Approaches defined above and others commonly used provide different ways to manage traffic issues. These strategies address problems with traffic management and get around those challenges. For example, ATSC handles traffic congestion in junctions through adaptive control and schedule, SDN solves the high volume of data and supports the different causes, and VFC addresses the communication problem. These strategies and several others open new avenues and methods for traffic management. However, the advancement of technology and continuous improvement in the infrastructure of the town to become a more inventive and more dynamic city requires a robust framework and higher data rates for sharing the sensors data that can support ultra-low latency (for warning, signals, transmits and receives data from its surroundings), scalability, and high reliability. Therefore, these approaches still need to be improved to overcome communication challenges.

5G wireless Network as a viable solution for Traffic management:

All of this is only conceivable when cities develop greater competence and intelligence and when the environment is capable of coordinated communication. Additionally, the advancement can only be possible with the progress of integration with wireless 5G networks that can support advanced intelligent transport systems, collect data, and securely communicate with other connected devices such as autonomous vehicles and V2X technology. Several features of 5G can potentially use these approaches intelligently, overcoming emerging cases and challenges in urban traffic management systems. Features that include ultra-low latency improving data transfer supporting the high volume of data, security, power consumption and network resilience are the core pillars of 5G that support traffic management and create new prospects for better advancement.

9.2 Health care

Each year, substantial advancements in healthcare are noted as a result of the digital transformation in the industry, which strengthens and improves observable differences and efficiency. The patient information system, lab results, appointment scheduling, prescriptions, and treatment data are just a few examples of the interconnected healthcare system.
The system can evolve to a certain point, and patients will profit from it by receiving a virtual assessment, education for patients, and access to healthcare information at any time. Patients can, for instance, view their test results online and further recommendations for their subsequent physician visits. In addition, several hospitals now permit patients access to their systems for educational purposes. So, they can get any detail online, such as the schedule for their exercise, the nutrition they need, and what to avoid during medications. Hence, every patient can access relevant information online at any time.

Lack of improvement:

- These developments nevertheless call for system improvements, such as two-way video virtual consultations, because it can be challenging for some elderly individuals to see a doctor or hospital. People must go even if they do not require physical procedures like routine checkups or early assessments to receive a specialist appointment.
- The processing of test results typically requires some time. As a result, patients are forced to hold off on taking their prescriptions until the test results are available and

their physician advises them to start taking their medications. The wait time makes the patient more anxious about their health, and some patients experience stress while they wait for days or weeks to receive their medicines.

- Surgeons are only accessible at their designated hospitals. One of the improvements we can notice in in-hospital treatment is the use of automated and robotic technologies, which are constantly growing. However, assistance from an expert or a surgeon, such as operating the machine remotely or operating from a remote place, must still be considered for effectively applying cutting-edge medical technology.
- For specialists to treat patients more effectively in an emergency and prepare before a patient comes, the ambulance service needs to progress in collecting patient data for healthcare staff, experts, or both.
- Patient monitoring can be improved; e-health devices are increasing. First, however, it must connect to the hospital system for real-time data, such as patients inside a hospital or even treated at any other location. Let us say the hospital system can gather and interpret monitoring data. In that situation, it can reduce treatment duration and increase effectiveness.

<u>5G Private wireless Network as a viable solution for healthcare</u>:

A private network can strengthen and make these technological developments more effective. With the service and deployment of a private 5G network, which can support and create many new options for the healthcare system's progress, the current healthcare improvement can be pushed and achieve a higher level. The above mentioned lack of progress can be fulfilled along with many others.

<u>Real-time high-throughput computational processing for diagnosis</u>:

Patient images and files are fundamental and crucial data in hospital care. The diagnosis reports and images such as MRI, CT-Scan, and X-ray data can now be transferred in real-time with a 5G network. First, it will save time, and physicians can diagnose and treat a patient with less time and help in accuracy, which further uses for rational decisions for efficient healthcare. Second, the 5G network can enable high bandwidth and low latency to process high-resolution data in real-time without delay to the server side or cloud that supports higher computing and processing images for further diagnoses. Finally, it can be processed quickly by a higher compute node on a server or in the cloud, saving individual clinics and hospitals money from purchasing local servers.

<u>Two-way video virtual consultations</u>:

Two-way high-definition video virtual consultation can be used for primary and secondary care, including routine check-ups, initial screening assessments, and rehabilitation sessions that do not require physical procedures. The high bandwidth, consistent quality and security of data and patient information and treatment can be possible with 5G private network deployment. It will reduce the cost and travel time to hospital visits for the patients. Also, specialists may take care of more patients, which reduces hospital and administrative expenditures.

<u>Real-time Patient Monitoring</u>:

5G enables the high-bandwidth and low latency. IoT and sensors can monitor the patients in real time, either in the hospital or at their location. Collecting data on hospitalized patients in real-time will reduce expenses for follow-up visits and improve the real-time decision for the physician and nurses for the next steps. Modern IoT devices can monitor fitness, food intake, sleep, or many other parameters, and real-time monitoring increases efficiency for doctor decisions. In addition to providing real-time monitoring for various metrics, IoT devices can also be used to gather data for artificial intelligence (AI) decision-making. Only the current state of wireless technological innovation made it feasible. Using the 5G wireless technology enables us to make use of it.

<u>5G enabled AR & VR in Health care</u>:

VR (Virtual Reality) and AR (Augmented Reality) are advancements in technology for healthcare systems such as remote surgeries, training, and rehab therapies. Starting from the first step, it helps and supports doctors, professionals, and surgeons to create an exact simulation of a patient body before the patient's actual treatment. Then, it advocates for the experiments or executes the complicated procedures to extrapolate the best way to treat the patient. Finally, in the continuity of the scenario, it supports doctors and surgeons to do remote operations if they cannot reach physically or some patients require some specialist support urgently, and physical specialists are not available.
Robotic-assisted Surgery (RAS) systems are getting involved in the healthcare system that combines robotic-assisted surgery with AR. This combination will improve the surgeon's ability to make real-time decisions. In addition, physical therapy and rehabilitation or behavioural treatment using AR will be more beneficial; it will increase patient engagement and data collection that allows the physiotherapist to evaluate and make a better decision for the patient. Furthermore, the data can be analyzed and supported to retreat the same type of patient, eventually adding value to the decisions using AI.

AR & VR require low latency that demands an awe-inspiring experience without lagging and high data transfer speed. It is possible through a private wireless network using 5G.

Other health initiatives: IoT Air quality sensors for Smart Environment Smart building:

Air quality directly impacts the health and well-being of residents and visitors within a community. IoT air quality monitors for indoor and outdoor use to track and manage air quality alerts and warnings. Emergency detection, such as fires or chemical spills, malfunctioning equipment, such as polluting automobiles, and air particulate quantity sensors can update equipment and facility maintenance plans for repair and alert guests on potential hazards.

Valuable information to support alerts and warning from IoT air quality sensors help to reduce the harmful impact on air quality and increase human health and the environment through specifying low-emitting materials—information such as carbon dioxide, carbon monoxide, ozone, nitrogen dioxide, total VOCs, formaldehyde.

These air monitoring sensors are outdoors in the city and indoors for buildings and get different data types in real-time. In addition, Interactive information such as alarms and warning to a user after processing is possible and implemented with fiber or 4G/LTE. A private 5G wireless network can effectively implement and manage evolving technology and an expanding number of devices, starting with the most sophisticated types of sensors and providing results in real-time.

9.3 Smart facilities

The technical transition, which produces and delivers new services, is a progression. Additionally, the enhancements in the facilities open unprecedented and endless opportunities to enhance customer experience, customize security and privacy, and have control over how facilities are managed. The combination of AI and IoT supports innovative facilities such as airports, shopping malls, and buildings that add value to their digital transformation roadmaps, take it to new customer experience with security, and manage it smartly.

Smart Building with Digital Twins:

The Digital Twins is limited without using a private 5G wireless network.

Issues:

Resource wastage for monitoring, security, temperature, and lighting in commercial buildings.

5G-enabled Smart Building with Digital Twins:

With IoT sensors and AI, the facilities are becoming more intelligent, changing the lighting and temperature in smart buildings. For example, in pathways, lights dimmer and brighten again when motion is detected; if there is no motion detection, lights in the room switch out. Likewise, the light will turn off automatically when building time is off, and no movement is seen.

The security team can monitor and guard the building remotely with IoT sensors, cameras, and AI. If the intruder is detected, there will be an alarm to the remote security person along with the site's video, and a specific camera switch to pop up on the security screen and follow the intruder's motion. In addition, security can move the robotic security dogs to inspect further if required or move to other steps like informing the city police. The processing in real-time with minimal lag and massive data from sensors and monitoring equipment to a consolidated central hub for control, such as a Digital twin platform, requires a 5G network privately.

Smart Waste Management:

One of the benefits we can achieve is waste management optimization by deploying the IoT and combining data collection and complex algorithms. Now we can achieve the most efficient waste management methods, such as waste collection, recycling the collected waste, and utilizing resources that reduce operating costs and increase the sustainability of waste services.

Deployment of IoT sensors and collection of data on waste collection areas, such as bins in residential areas, commercial areas, and construction sites, can help collectors and recycling companies. For example, a Digital twin waste management is a virtual digital copy of garbage collection. It triggers that result after applying algorithms in the gathered data can support in many ways for optimizing the process.

- optimization & increase in sustainability.
- re-use of waste material
- optimal processing
- optimal pickup routes for collectors
- reduction of expected waste streams
- Reducing the workforce

Benefits:

Fewer routes or pickup collectors can save costs and emissions by reducing fuel consumption and help in reducing traffic congestion.
Recycling waste material can achieve in efficient ways. For example, different IoT sensors and intelligent monitoring systems can help to split the recycling material (the most common raw material for industrial).
Analytics data can support the placement of bins more effectively, optimizing the process more and making the environment healthy.
Supporting and working GPS inside waste collection vehicles can show the best route to collect data and only shows from where to gather.

5G-enabled Digital Twins Waste Management:

Smart waste bins using IoT sensors, recognition technology, and AI enable trash to be automatically sorted for raw material or analyze data that can optimize the entire process and digital twin waste management that is a virtual digital copy of the waste management; all of this requires 5G deployment that can support a significant number of IoT devices and provide real-time results.

Smart Logistics:

IoT in transportation, such as logistics, shipments, deliveries, and warehouse operations, has been expanding. In addition, the industry is driving forward with autonomous vehicles and benefits from advanced technologies.

Autonomous Vehicles on the Road delivery and operation:

An autonomous "POD" is a fully driverless electrical vehicle in many cities worldwide. 5G enabled POD can use on the road for delivery, such as delivery truck POD or public transport in any public area, such as an airport or any different operations. A POD is equipped with numerous sensors and cameras for operations. In most places, it uses on-demand and operates along predetermined routes. Collecting data in the control center for optimal operations & analytic purposes is the way to move forward, and POD can be used in extended ways. The central hub for operations can control with AI and algorithms that help advance the technology for POD and enable efficient use of the technology in any route like POD taxi and POD delivery on the road.

5G enabled Autonomous Vehicles:

IoT, sensors, high-definition cameras, and autonomous vehicles using analytical data and algorithms must process with low latency and high data rates. A private wireless network of 5G enables us to fulfil the demand for completely autonomous vehicles.

Use Real-time Image Processing in Traffic:

Use Real-time Image Processing in Traffic to Track Down Scofflaws & data collection to track history is one of the advancements in technology. This automated license recognition system is in operation in many cities. For example, ALPR (Automated License Plate Recognition) in Waterloo, Ontario, was used by police to detect license plates in real-time from cameras mounted on top of a police vehicle. The cameras on the top continuously scan license plates to detect a vehicle in poor standing, such as a driver with a suspended license, suspended license Plates, expired validation tags, and reported missing or stolen vehicles. The ALPR system is capable of scanning thousands of license plates per hour. However, it does not record any plates or videos or save them in the central hub for tracking purposes. It also does not work for moving violations like speeding, crossing at red lights, or accidents.
The other example in UAE by Dubai police using ANPR (Automatic Number Plate Recognition), the same type of function used by the police and model is same including parking lot tickets or detecting no parking zones.

9.4 Augmented Reality

AR in Medical:

Every year, the complexity of surgical procedures increases, placing more pressure on surgeons as new surgical specialties are added. As a result, AR (Augmented Reality) is rapidly gaining popularity in the medical area.
Workflow of the surgeries using technologies connected with data such as complex process information, patient information in real-time and processing and suggestions for the best way to proceed in the procedure's subsequent steps., including the data visualization through AR, for example, visualize surgical 3D data on AR device. In addition, during surgeries with AR support, surgeons visualize 3D models of image scans such as x-rays or MRIs in real time. It involves

several Giga Bytes of data that need to be rendered & processed in real-time and ready for the surgeons to visualize in 3D with AR. In addition, it needs accuracy and low latency, which all require a 5G private wireless network to implement the advancement in the technology.

AR in Operations & Maintenance/repair:

The most prevalent use case for augmented reality is repairing or maintaining any active device in operation with connected data or customer impact. Operation and maintenance are regular tasks in many engineering/non-engineering fields. Generally, the maintenance team or individual can perform maintenance following the equipment's schedule and design. They carry out the activity according to predetermined procedures or a workflow. However, if it creates another issue during the process, they need to work out to figure out and address the underlying problem. The team or individual can efficiently do the maintenance using AR technology when combined with relevant procedures and data for that particular device, including historical problems and repair or maintenance data in real-time. For example, if a device has an issue and repair that need extra care for the time being or if there is a problem that another person has already entered into the system or notes that indicate to be aware or broken part indication can easily be accessible to the maintenance team in real-time. The equipment design and workflow in AR devices do planning for device maintenance and repair simple, taking less time. The design, workflow, processes, and related data connected and accessible to AR reduce resources, planning and errors/mistakes during maintenance and operations.

9.5 Security & Smart Mobility

Public Safety and Security:

Security and safety are essential elements of the community, and intelligent infrastructure can support those needs. For instance, noise sensors detect gunshots, screams or cries for help, and other crisis indications.
IoT sensors connected to a surveillance system generate location and live video alerts for efficient, immediate emergency response. The installation of these sensors in sensitive areas, clubs, private parties' areas, and pubic areas such as airports, and train stations, along with surveillance that is connected to a central system and mobile security team, will not only promote immediate emergency response but also support monitoring and analyses with AI to calculate risk and mitigate everyday situations.
The vast amount of data that needs to be transferred and processed after analyses along with image processing or real-time video to a centralized hub and mobile team, such as a security vehicle monitoring system near that location, requires high speed to transfer the data and low

latency to act efficiently. It can be achievable by implementing a private 5G wireless network for the community.

First Responder Support-Smart Mobility:

A first responder system for incident Management software where the road network monitoring in a real-time surveillance system, connected with two-way emergency communication on the roadside and Smart mobility and digital hubs such as for drivers witnessing incidents or anyone besides the incident location can report them via the designated mobile application supported by government or community to the public for their reporting. An efficient and robust first responder can be implemented with these connected multiple services and sensors in real-time that quickly support response and clear the road condition at the scene of the incident location and traffic.

Public safety and tranquillity management:

Smart poles are commonly used in smart cities that are equipped and provided with multiple services such as intelligent surveillance systems to monitor crowd management, noise sensors, two-way communication for emergency support, weather conditions, air pollution, signage digital connection with a central system that can alert for safety and tranquillity management. Fiber-connected smart poles are currently implemented. However, the growth in urban population and the development of wireless connectivity necessitates smart poles that can connect to mobile security vehicles for efficient performance and be installed anywhere. 5G wireless networks provide numerous advantages and more effective ways to execute these developments.

3. Conclusion

Working with a Private wireless network like the 5G has several benefits. First, the original hype surrounding smart cities has subsided with applications moving past early pilots and proofs-of-concept into commercially deployed systems. Several towns have constructed wireless networks for their Smart City and public transit projects.
The private wireless network's ultra-high reliability helps to avoid costly and frequently hazardous downtime. Ultra-reliable communications are necessary for mission-critical uses. Another essential advantage and requirement for mission- and business-critical applications is predictable performance. There should be constant high data rates, minimal latency, and rapid, secure response times for linked people, equipment, and applications. The capacity to support even the most demanding command-and-control applications is added by ultra-low latency.

Cities can benefit from private wireless solutions to boost next-generation automation, guarantee security and safety, and boost productivity. The control of traffic congestion, emergency vehicle guidance, and the addition of support for connected and even autonomous buses are all Smart Cities efforts that put heavy demands on current or potential wireless networks. However, these initiatives will benefit from improved safety, effectiveness, and rider satisfaction that can now be achieved from a private wireless network.

A cutting-edge, sizable, high-performance infrastructure project, the intelligent city private network partnership will bring enhanced and completely controlled digital 5G connectivity to the city to benefit the town, its residents, and tourists.