TATA COMMUNICATIONS

TATA

A GUIDE TO ENTERPRISE CONNECTIVITY SOLUTION

TABLE OF CONTENTS

1 Scope of the Paper

Scope of this paper consists of comparison of different connectivity solutions for industry4.0. We will discuss various connectivity solutions for industrial need. There exist different technologies and each technology has its own merits and demerits.

The challenge today is that enterprises often deploy several types of connectivity solutions, each linked to a specific application or use case, and therefore must manage the complexity of having fragmented systems and a large number of interfaces. This also results in a higher overall total cost of ownership.

So an enterprise needs to choose right technology fit which can meet its requirements and enable next gen use cases.

2 Different Connectivity Technologies

As the technology is evolving and has evolved from its predecessors, for an enterprise there are multiple connectivity options available for connecting different devices.

We started in 90's with Wi-Fi and Cellular technology as two different means of wireless connectivity solution. Over the years, lots of development and innovation has taken place in next generation of Wi-Fi and Cellular technologies to meet the demand of ever evolving different use cases.

In Wi-Fi, we started with 802.11ab in late 90's and in cellular technology GSM. Over the years Wi-Fi standards have evolved from 802.11ab to 802.11a/g, 802.11n, 802.11ac and latest release 802.11ax or Wi-Fi 6.

Similarly cellular technologies have evolved from GSM (2G) to 2.5G (EDGE) to 3G to 4G to latest 5G.

Each release comes up with enhanced and new features integrated to cater the requirements of industry 4.0 use cases. Advancement in technology opens up new and unimaginable use cases. These use cases later on prove to be a catalyst in operational efficiencies and new revenue streams.

Both Wi-Fi and Cellular technology have their own characteristics and strengths, thus both sometimes compete to each other and sometimes complement each other.

In this paper we will talk more in detail about the two latest technologies Wi-Fi and 5G, how both are different to each other, and subsequently which version is more optimal solution for connectivity and in what scenario.

3 Introduction to Wi-Fi

Wi-Fi is a set of wireless protocols based on IEEE 802.11 family of standards. It mainly operates on 2.4 GHz and 5GHz ISM bands that require no licensing. Wi-Fi is a trademark of the non-profit Wi-Fi Alliance.

Over the years, most of the enterprises have been deploying Wifi technology for its wireless connectivity needs.

The most common Wi-Fi standards being used in various applications are 802.11a, 802.11b, 802.11g, 801.11n (also known as Wi-Fi 4), 802.11ac (Wi-Fi 5), and 802.11ax (Wi-Fi 6).

Below table depicts the different specifications and advancements in different releases. There is significant change in max data rate, supported modulation scheme etc.

Standard / Feature	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
First available	1999	1999	2003	2009	2013	2016
Max data rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	6.93 Gbps	9.6 Gbps
Frequency band of operation	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz and 5 GHz	2.4 GHz and 5 GHz	2.4 GHz, 5 GHz and 6 GHz for 6E
Channel width	20 MHz	20 MHz	20 MHz	20/40 MHz	20/40/80 MHz,160 MHz and 80+80 MHz (optional)	20/40/80 MHz,160 MHz and 80+80 MHz (optional)
Number of spatial streams	1	1	1	Up to 4	Up to 8 with SU-MIMO and MU- MIMO (downlink)	Up to 8 with OFDMA and MU-MIMO
Modulation	BPSK, QPSK, 16-QAM, 64-QAM	CCK/DSSS	CCK/DSSS/ OFDM	CCK/DSSS/ OFDM	BPSK,QPSK,16-QAM, 64-QAM and 256-QAM (optional)	BPSK,QPSK,16QAM, 64QAM and 256QAM, 1024QAM
Average indoor coverage*	115 ft.	125 ft.	125 ft.	230 ft.	230 ft.	98 ft.

The equipment, both access points and end devices, often support multiple standards simultaneously. The standards that came later are backwards compatible with earlier standards with some caveats. For example, an 802.11ac router can work with a mobile set supporting the 802.11n standard. However, during communication, both the access point and end device must use a common standard.

Actual coverage depends on multiple factors including relative positions of transmitting and receiving antennas, antenna gain, size, and location of obstructions in the line-of-sight, and frequency of operation. Under identical circumstances, 5 GHz signals have higher attenuation (hence, lower reach) compared to 2.4 GHz signals.

There are multiple types of Wifi usage:

Office use: Wifi is predominant technology for office use where there is almost no mobility. Employees use Wifi for their office work from laptops, Handsets etc.

MSME business: small and medium scale businesses use wifi not only for underlying connectivity for its employees but also to connect some of their endpoints which are in operation for their business needs. Example- POC machines, bar code scanners etc.

Manufacturing units: Manufacturing units generally have lots of complex machines, robots and production lines. These robots and machines are connected with wifi. It is very essential in such industries to closely monitor the performance and production of these machines. Any unintended breakdown may results in loss of production. So network reliability is one of the major requirements in such scenario. WiFi, to some extent provide this reliability in static scenarios where there is no mobility involved.

Large Scale businesses such as Ports/Mines: Typically, large scale businesses which span across a wide area do not get much benefit of Wifi Generally, these kinds of enterprises rely on public connectivity.

4 Wi-Fi Benefits

4.1 Convenience

Through a wireless network, multiple users can connect with the router or through a hotspot technology without any configuration required. This gives you ease of use and access to the available network. Linking to such a network takes a few seconds. This capability to connect through a wireless network literally supersedes the wired or cable network, which takes more time to configure and allow connection in a multi-user environment.

4.2 Mobility within the office

An internal Wi-Fi network means the end of the requirement for employees to remain tethered to their desks. Internal Wi-Fi allows employees to work at their desk, in a conference room, or in any other location.

There is seamless mobility under one access point, however if there are multiple access point deployed in the premises, Inter access point mobility is not possible.

4.3 Multiple connection support

Wi-Fi Supports Multiple Connections. It supports around 30 devices simultaneously. It may not provide multiple connections options like LAN or other wired technologies which can provide connections for more than 100 devices.

But the multiple Wi-Fi Connection doesn't need hundreds of cables. You won't need to bother about the connectivity types of each device.

4.4 Increased opportunity

Wireless Technologies provide more opportunities for manufacturing and development companies. Wi-Fi devices provide more opportunities in developing IoT-related products.

5 Wi-Fi Major Challenges

5.1 Unsuitable for outdoor environment

Range of Wi-Fi is very low which falls below 100 feet. For industries operating in large indoor areas or outdoor areas, Wi-Fi has a challenge to be deployed due to number of required access points to meet the requirement.

5.2 Security challenges

Security concerns have held back Wi-Fi adoption in the corporate world. Hackers and security consultants have demonstrated how easy it can be to crack the current security technology known as wired equivalent privacy (WEP) used in most Wi-Fi connections. A hacker can break into a Wi-Fi network using readily available materials and software.

Although Wi-Fi comes with its own benefit, security has been one of the major deficiencies in Wi-Fi, though better encryption systems are now becoming available. Encryption is optional in Wi-Fi. An unsecure network is like leaving your home and all of the contents inside it open and vulnerable to burglary and theft.

Three different techniques have been defined. These techniques are given here

5.2.1 Wired equivalent privacy (WEP)

An RC4-based 40-or 104-bit encryption with a static key. Developed in 1999, Wired Equivalent Protocol (WEP) was the only security protocol available for early 802.11a/b devices.

5.2.2 Wi-Fi Protected Access (WPA)

After severe vulnerabilities in this protocol were exposed in 2001, Wi-Fi Protected Access (WPA) was introduced by Wi-Fi Alliance in 802.11g devices. Future 802.11b/g devices also supported WPA. WPA had two modes – WPA Pre-Shared Key (WPA-PSK) or WPA Personal for home networks and WPA Enterprise for enterprise networks. WEP used static 64-bit or 128-bit encryption keys whereas WPA, through Temporal Key Integrity Protocol (TKIP), uses per-packet based 128-bit key.

This is a new standard from the Wi-Fi Alliance that uses the 40 or 104-bit WEP key, but it changes the key on each packet. That changing key functionality is called the Temporal Key Integrity Protocol (TKIP).

5.2.3 IEEE 802.11i/WPA2

The IEEE is finalised the 802.11i standard, which is based on a far more robust encryption technique called the Advanced Encryption Standard. The Wi-Fi Alliance designate products that comply with the 802.11i standard as WPA2.

In 2004 WPA2 replaced WPA. WPA2 features stronger cryptography than earlier two security protocols and uses Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) and it uses 128-bit Advanced Encryption Standard (AES). However, implementing 802.11i requires a hardware upgrade.

5.2.4 WPA3

In 2018, Wi-Fi Alliance introduced WPA3 as a replacement of WPA2. WPA3 uses 192-bit encryption key compared to 128-bit in its predecessor. This protocol aimed to mitigate security issues posed by weak passwords and ease the process of configuring devices with no display interface.

5.3 Compatibility and Interoperability

One of the major problems with Wi-Fi is its compatibility and interoperability. For example, 802.11a products are not compatible with 802.11b products. Due to different operating frequencies, 802.11a hotspots would not help an 802.11b client. Due to lack of standardisation, harmonisation, and certification, different vendors come out with products that do not work with each other.

5.4 Mobility Issues

As the client moves away from the AP to which it is connected, the strength of the signal decreases and RF interference in the area generally increases. Due to the decreased signal strength and increased interference, some transmitted data packets are not received, forcing the sender to retry the transmission. To maintain the Wi-Fi connection, the client and AP negotiate a lower data rate. If the client continues to move away from the AP, then it eventually reaches the edge of coverage for that AP, where the Wi-Fi connection can be maintained only at the lowest data rate supported by that AP. Beyond the AP edge of coverage, the client is out of range, and the connection with the AP is lost. Therefore, to prevent loss of coverage, the client will switch to an AP with stronger signal, after disconnecting from original access point. Mobility in Wi- Fi is break before make, hence mobility is not seamless between two access points.

5.5 Lower Range

The Range of WiFi is limited. One cannot use Wifi if two devices are at a long distance apart. WiFi Range is limited to Under 100 feet.

As the Range from the Host Increases the speed decreases. The speed of WiFi is inversely proportional to Range.

It is also not good for use between larger rooms.

5.6 Network management Issues

It's very difficult to manage high no of Wi-Fi access point centrally as each access point behaves as a standalone NW. Centralised monitoring is a major challenge.

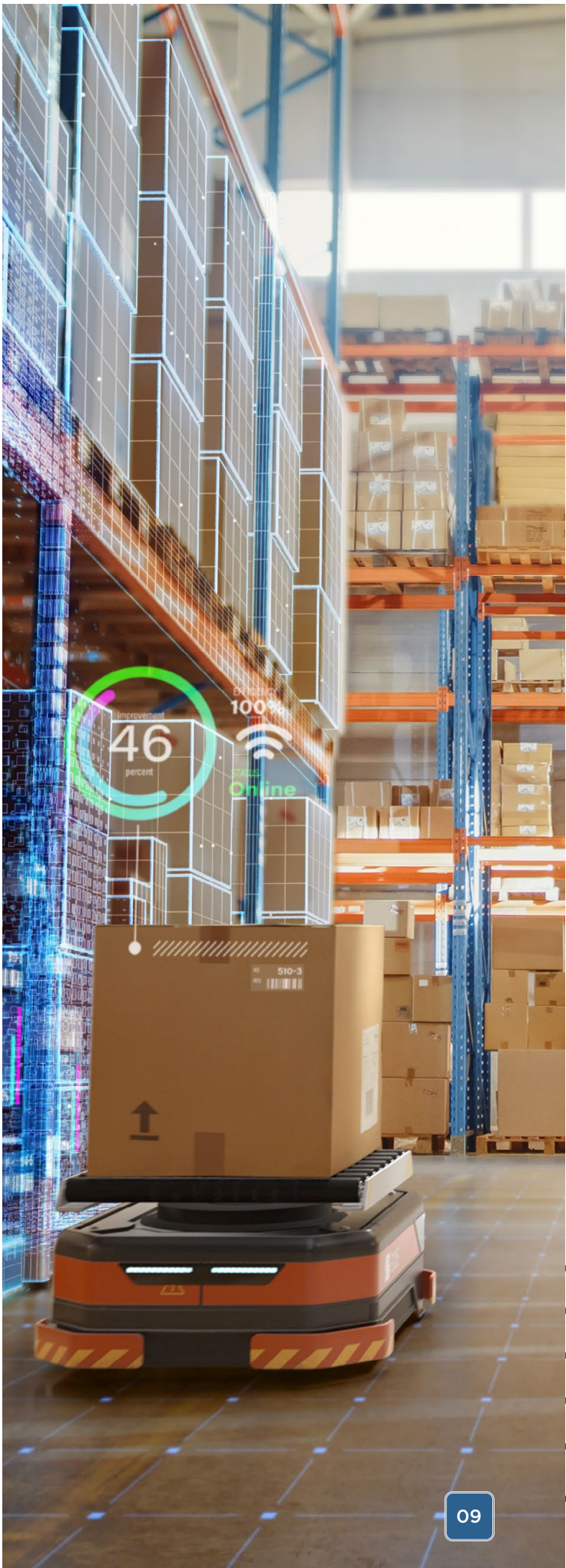
6 Wifi Summary

As detailed in previous sections, Wifi is an important technology for enterprise connectivity. Most of the enterprises be it small, medium or large have already deployed Wifi in their campuses. Wi-Fi is currently the backbone of their network along with wireline connectivity.

There are some of the inherent advantages of Wi-Fi in certain scenarios like indoor, low mobility scenario. For such applications Wi-Fi would always be first choice.

While Wi-Fi has huge foothold in the enterprise market, it is less focussed on vertical use cases such as manufacturing, retail, ports, mining, campus network, AR/VR/XR etc. There is very less talk about Wi-Fi for a particular sector specific solution.

Depending upon enterprise type, usage, application drives the adoption of Wi-Fi.

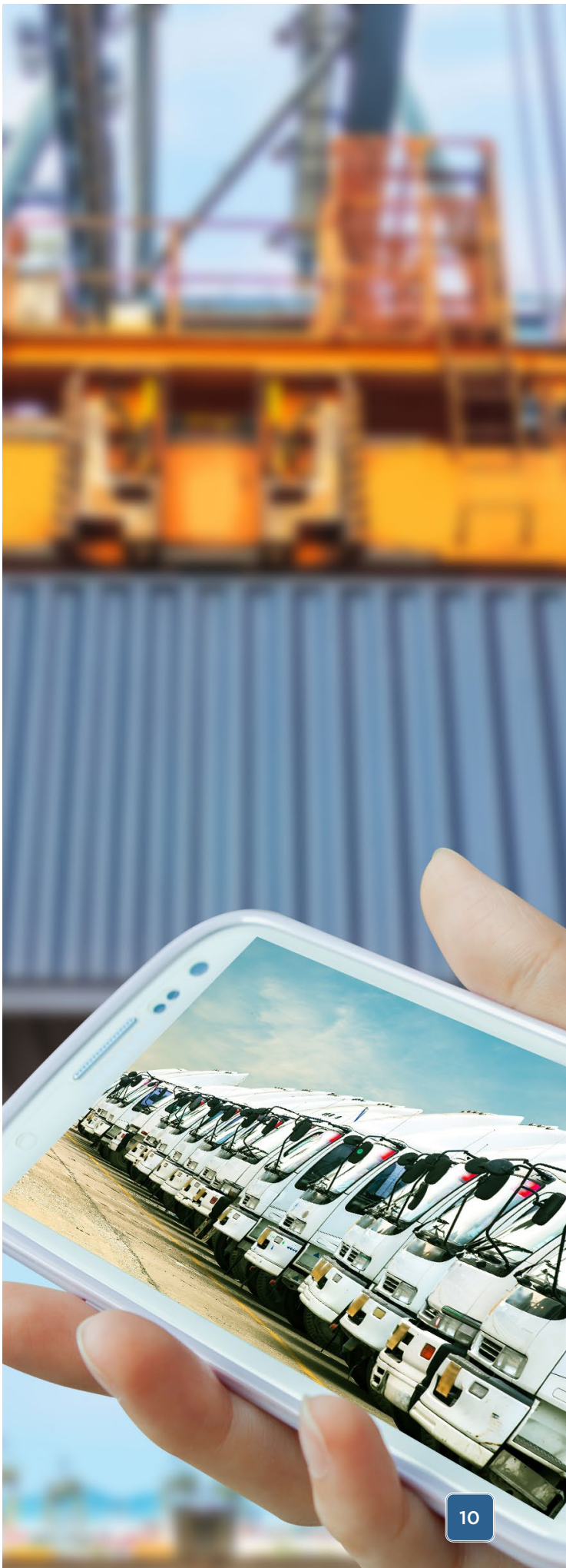


7 Cellular Technology for Enterprise Connectivity

Private LTE solutions have increasingly been deployed in manufacturing, mining, ports, campuses, and other large enterprise operational sites. A private LTE network uses dedicated spectrum as well as dedicated operating functions and/or assets. For example, the radio, core, and management functions can run on the enterprise's own infrastructure or can run off infrastructure that is shared. Private LTE can use licensed, unlicensed, or shared spectrum. Licensed spectrum is provided by mobile carriers, unlicensed spectrum can be accessed by anyone, and shared spectrum is spectrum that is licensed but shared (e.g., CBRS).

There are clear security and reliability advantages to operating your own private cellular network which make private LTE attractive to security-sensitive and/or mission critical industries such as defence, manufacturing, and extractives.

The capabilities of private LTE over Wi-Fi may make it tempting for many businesses.

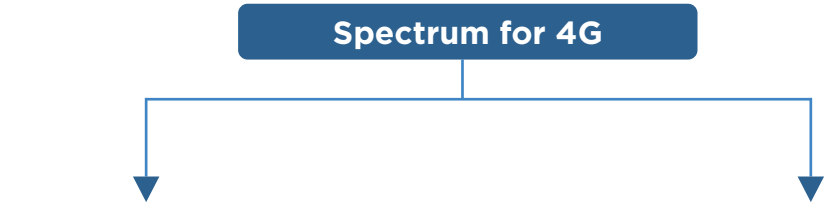


Comparison	2G	3G	4G	5G
Introduced in year	1993	2001	2009	2018
Technology	GSM	WCDMA	LTE	MIMO, mmWaves
Access System	TDMA, CDMA	CDMA	CDMA	OFDM, SC-OFDM
Switching Type	Circuit switch for voice Packet switch for Data	Circuit switch for voice Packet switch for Data	Packet switching for both voice and Data	Packet switching for both voice and Data
Network Speed	<20kbps	40mbps	300mbps	>2Gbps
Channel Bandwidth	~5MHz	5-10MHz	Up to 20MHz	Up to 100MHz for mid band Up to 400MHz for mmwave
Advantage	Multimedia features (SMS, MMS), internet access	High security, international roaming	Speed, high speed handoffs, global mobility	Extremely high speeds, low latency, machine to machine connectivity
Application	Voice call, Short messages	Video conferencing, mobile TV, GPS	High speed applications, mobile TV, wearable devices	High resolution video streaming, remote control vehicles, robots, AR-VR etc.

In this paper we will discuss primarily 4G and 5G technologies which offers higher data connection speed.

7.1 Spectrum requirement for 4G and 5G

4G and 5G can operate in in both licensed and unlicensed spectrum bands. Below picture shows how 4G and 5G spectrum is currently awarded to different institutions globally.



Licensed Spectrum

- Administered by local regulatory body
- Generally awarded through bidding process
- Most of the case applies for unified license across large territory
- Typical band
- 4G-600/700/800/900/1800/2100/2300/2500

Unlicensed Spectrum

- Administered by local regulatory body through relaxed guidelines
- Anyone can operate in unlicensed bands with complying to local regulations
- Can be deployed in localised area
- Typical Bands
- 4G-U/LTE-U-5.1-5.8GHz

Spectrum for 5G

Licensed Spectrum

Unified License

- Administered by local regulatory body
- Generally awarded through bidding process
- Applies to large territory mainly MNOs
- Called Public Networks
- Typical Bands
- 5G-3.3-3.6GHz,3.7-4.2GHz,24.2-52.5GHz

Local License

- Administered by local regulatory body
- Spectrum reserved for local or captive use only.
- Applies to small territory mainly industries
- Called Non Public Networks or Private Networks
- Typical Bands
- 5G-Each country has different guidelines

Unlicensed Spectrum

- Under consideration by 3GPP in Release 17
- Typical Bands -5.1-7GHz

7.2 Private LTE as enterprise connectivity solution

Private LTE solutions have increasingly been deployed in manufacturing, mining, ports, campuses, and other large enterprise operational sites. A private LTE network uses dedicated spectrum as well as dedicated operating functions and/or assets. For example, the radio, core, and management functions can run on the enterprise's own infrastructure or can run off infrastructure that is shared.

Private LTE can use licensed, unlicensed, or shared spectrum. Licensed spectrum is provided by mobile carriers, unlicensed spectrum can be accessed by anyone, and shared spectrum is spectrum that is licensed but shared (e.g., CBRS).

There are clear security and reliability advantages to operating your own private cellular network which make private LTE attractive to security-sensitive and/or mission critical industries such as defence, manufacturing, and extractives.

The capabilities of private LTE over Wi-Fi may make it tempting for many businesses.

7.2.1 Private LTE in Licensed Bands

As we saw from earlier sections of the paper that LTE can be operated in both licensed and unlicensed bands. Generally, ownership of licensed band lies with successful bidder so if an enterprise wants to deploy its own network, then it must procure spectrum from local MNO.

Since ownership of spectrum lies with MNO, Enterprise has to follow MNO's way of deployment. So directly or indirectly enterprise has Partial / No control over its own network.

Overall TCO of setting up a private network in licensed band tends to be high due to high spectrum fee.

7.2.2 Private LTE in Unlicensed Bands

Other option to deploy a private network is in unlicensed band i.e 5.1-5.8GHz. This band has been designated by 3GPP and WRC for unlicensed operations.

Compared to licensed bands, deploying LTE in unlicensed bands is much easier. An enterprise can choose a system integrator of its own choice and can deploy customised network for its own use case.

Since spectrum ownership lies with enterprise itself, Flexibility is there in deploying and managing the network.

Enterprise can configure network its own way to meet the end use case requirement.

8 Benefit over Wi-Fi

LTE is an 3GPP cellular technology. Weather you operate in licensed band or unlicensed band, underlying 3GPP feature remains same.

Ease of deployment: Coverage of LTE-U is higher than Wi-Fi, So one needs less no of Radios compared to no of Wi-Fi access point for same area of operation

Security: Unlike Wi-Fi, LTE is much more secure.

Mobility: Any of 3GPP technology 4G/5G supports seamless mobility. They work on the principal of make before break.

Larger Coverage: LTE has better coverage than Wi-Fi and a suitable option for outdoor deployment. Enterprises for example ports, mines, manufacturing plants etc which operates in large areas need seamless and ubiquitous coverage, for such enterprises LTE is one of the best options.

9 Challenges in LTE-U

Interference: Since LTE-U operates in unlicensed bands, there are higher chances of interference since these bands are not harmonised. Chances of interference is there.

Ecosystem readiness: OEMs, ODMs have started lately investing in LTE-U development. End device readiness is a challenge in LTE-U.

9.1 Private 5G as enterprise connectivity solution

The main distinction between commercially available 5G and private 5G networks is that organisations own every part of their private 5G network. Similar to enterprise Wi-Fi, private 5G networks have complete control over their network resources, and how those resources are distributed.

Private cellular networks allow operators to granularly control their network resources, meet the exact latency and throughput requirements. Rules can be set and synchronised for specific applications, groups, devices, and subnets across enterprise environments.

This is also the case for private LTE networks that don't have 5G access quite yet. The same rules and principles apply to private LTE networks, just at 4G levels of performance. Organisations that already use private LTE will find it much easier to upgrade to private 5G in the future.

Private 5G will deliver lower latency and higher bandwidth, reliability than previous iterations of mobile technology. Industries want to implement value-adding use cases that was not possible before.

Private 5G improves on private LTE in several areas, including higher bandwidth, mobility, and lower latency, and can support a much greater density of devices. These improved capabilities enable new use cases and significantly augment others, such as Autonomous Mobile Robots (AMRs), AR/VR/MR, wireless robots, and drone or UAV inspections or repairs.

However, in many cases, private LTE can be more than sufficient to meet enterprise requirements and has already been doing so in industries such as mining and ports. Therefore, it is important for enterprises to ensure that they really need the capabilities that private 5G brings

9.1.1 Dedicated spectrum for Private 5G

With increasing demand from various industries and new use cases with 5G, many countries have started setting aside some chunk of frequencies dedicatedly for enterprises.

For example- Germany, UK, US, Malaysia etc have dedicated spectrum for non-public network (Private Network)

Below figure shows the no. of countries which have opened different options to enable CNPN by means of setting aside dedicated spectrum or through TSP leasing

Mid band

Brazil, Chile, China, Croatia, Czech Republic, Denmark, Finland, France, Germany, Greece, Japan, Netherlands, Norway Poland, Republic of Korea, Sweden, Taiwan, UK, US

Source: Ericsson

High band, mmW

Australia, Denmark, Finland, Germany, Greece, Hongkong, Japan, Republic of Korea, Sweden, Uk

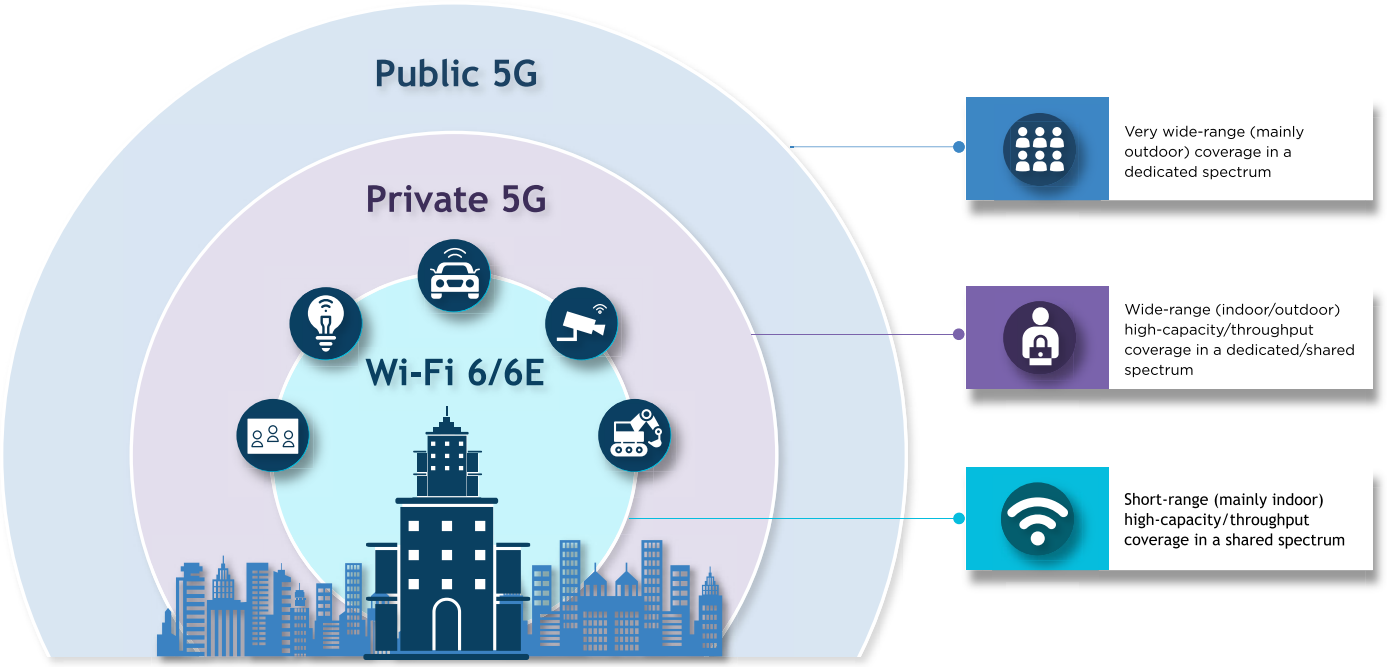
10 Comparison between Wi-Fi,LTE-U and Private 5G

Depending upon different use cases and area of deployment, each technology has its own merits and demerits.

It's important to understand that unlike many other sofware-based technologies, choosing a connectivity technology is not a straight-forward process since it depends on a variety of factors:

- **Network availability (in the area of deployment), uptime and SLA**
- **Expected data through-put**
- **Range and mobility**
- **Frequency of data transmission and device battery life**
- **Acceptable latency limit**
- **Data Security and compliance to local regulations**
- **Use case and device support**
- **Possibility of Remote updates**

This section describes the key differentiators while choosing the technology for connectivity.



	Bandwidth	Low Latency	Indoor Coverage	Outdoor coverage	Mobility	Security and Privacy	IT/LAN Integration	Interference Risk	Intl. Spectrum	Device availability
Wi-Fi 4/5	✓	✗	✓	✗	✗	✓	✓✓	✗	✓✓	✓✓
Wi-Fi 6/ 6E/7	✓✓	✓✓	✓✓	✗	✓	✓✓	✓✓	✓	✓	✓✓
Private LTE	✓	✗	✓✓	✓✓	✓✓	✓	✓	✓	✓✓	✓✓
Private 5G	✓✓	✓✓	✓✓	✓	✓✓	✓✓	✓✓	✓✓	✓	✓
Public 5G	✓	✓	✗	✓	✓✓	✓	✗	✓✓	✓	✓
Fibre/ ethernet	✓✓	✓✓	✓	✗	✗	✓✓	✓✓	n/a	n/a	n/a

Source: STL Partner

11 Summary

The question of Wi-Fi and cellular technology, difference and applicability has been there since many years. While Wi-Fi was primarily started to connect homes, small offices, low mobility areas, cellular technology coexisted and gave a fierce competition.

It's been more than 15 years now, we see in some scenarios both technologies compete with each other while in some they complement each other.

For a lot of organisations, focus has moved from connecting employees, laptops, handsets to connecting machines, IoT, cameras, proving high end use case applications.

The advent of 5G with enhanced features like eMBB, uRLLC and mmTC and specially private 5G,, enterprises can now focus on deploying advance systems with autonomous vehicles and robotics. 5G is more capable of handling such applications due to it's ability to slice the network and provide necessary bandwidth to each application without interrupting the other applications.

Most industrial uses for PLTE/P5G actually involve replacing other technologies such as fibre or private radios, rather than Wi-Fi, except in certain specific settings such as warehouses. Other industrial networks are for mid/wide-area deployments such as utility grids, airport ramps or oilfields, which are not Wi-Fi strongholds anyway.

An enterprise needs to keep in mind certain scenarios to decide the right technology for its use case. Below are some of the listed key decision makers:

Indoor Vs Outdoor

One need to thoroughly evaluate the area where connectivity is required. If its indoor only area with static end point deployment Wi-Fi makes the choice while if the deployment area is large and outdoor, Private 5G becomes the first choice.

Use case applications

If use case applications need low latency, involves mobility and high reliability the private 5G is the choice. If there is no such need and only plain vanilla flavoured connectivity is required the Wi-Fi can be adopted.

Next generation use cases

As technologies are growing at a very rapid pace, new use cases which were unimaginable a decade ago are now available commercially in the market. AR/VR/MR is one such example. Considering the evolution of use cases and applicability in the enter prise area, one should chose Wifi or private 5G.

Vehicle applications

Vehicles and other moving devices (robots, drones, etc.) are increasingly equipped with cellular radios, especially if they operate on public roads as well as on-site. While they may use Wi-Fi as well (especially indoors), they are important use cases for the future of CBRS and PLTE/5G

Device connectivity

There are many Wi-Fi only devices, these devices can also benefit from private cellular technology, by using a local gateway / hotspot (CPE- customer premises equipment) that connects to 4G/5G with a secondary Wi-Fi connection for nearby devices.

Device / User per sq meter

In recent years we are seeing everything getting connected to internet. Device and user density has increase multi folds over the years. So is the scenario in enterprise network. New devices have been introduced for better quality inspection, manufacturing robots etc.

Keeping user density in mind one has to choose Wifi or cellular technology as Wi-Fi is known for less no of device connectivity density.

Security

There are many industries which deal in high security businesses, for them security is the topmost priority. Wi-Fi has been vulnerable to security threats since its inception. For these kinds of enterprises Private cellular technology should be the first choice while those which are in business where even low security is acceptable, Wi-Fi can be adopted.

To summarise, we see that both Wi-Fi and Cellular technologies working in conjunction to provide a seamless experience. One should select on the basis of requirement and use cases.

For more information, visit us at www.tatacommunications.com

CONTACT US