WHITE PAPER

Industrial IoT in a 5G world - Architecture

aruba
a Hewlett Packard
Enterprise company

ABSTRACT

An Industrial IoT system is a complex architecture encompassing sensors, communications, big-data storage, edge computing and advanced analytics among its disciplines. In the communications segment, the 'last hop' for Industrial IoT is now wireless wherever possible, driving cost saving, increased flexibility and greater mobility than wired connections. When considering the last hop, a key question, which we will investigate in this paper, is which wireless technology to select. For large-scale Industrial IoT networks, the viable technologies are variants of the Wi-Fi used in enterprise networking today, and 4G from public cellular networks.

The paper examines the architectural strengths and weaknesses of each technology in the network models used today, comparing Wi-Fi 5 with public and private 4G architectures. It also covers the emerging Wi-Fi 6 and 5G technologies as they will become available to the Industrial IoT market in the near future.

EXECUTIVE SUMMARY

This paper considers the wireless network used to connect IoT devices to the computing and storage resources needed to build a full IoT architecture. While these latter elements are more complex (and expensive) than the network, the paper only considers the edge networks large organizations require for Industrial IoT purposes. Even industrial and plant IoT is a broad market and includes many environments; this paper is applicable to scenarios including factory automation, chemical plants, oil refineries, oil exploration and production sites and mines.

Industrial IoT is part of OT (Operational Technology), a different domain from IT (Information Technology). For CIOs and the IT ecosystem, cybersecurity and trustworthy data are top priorities, and device and network outages are tolerated for security and operating system vulnerability updates. But COOs, responsible for OT, prioritize plant availability and manufacturing output targets. This drives a different mindset when managing the network. For example, security updates and OS patches are anathema to both targets and must be very carefully scheduled and implemented. In this paper we emphasize those technology aspects that are important to OT.

This diversity of site geography drives wireless topology requirements including range, radio mounting points, power and backhaul, and options to reach mobile as well as static IoT devices. Other requirements are derived from specific IoT applications. In this paper we consider low-rate instrumentation for temperature, pressure, vibration and other telemetry, and also imaging and video monitoring, with requirements ranging from low-resolution video surveillance to very high-speed interactive video for real-time control and augmented reality applications. Traffic requirements include low-to-high data rates and differentiated quality of service treatment including prioritization on shared infrastructure, latency and jitter. Finally, security is an over-arching requirement that plays a significant role in wireless network technology and design.

While many wireless standards target 'Industrial IoT', including PROFINET, Wireless I/O, ISA100, wirelessHART, LoRa and others, only Wi-Fi and cellular 4G/5G span the network scale, traffic capabilities and diverse topologies required for the networks defined above therefore, the paper focuses on these technologies. It categorizes four different network models, one with Wi-Fi and three that use variants of cellular technology. It is important to specify the deployment model, because while cellular technology and Wi-Fi each have advantages in certain architectures, these advantages are network-architecture-dependent, and are not available in all network models.

Wi-Fi networking for Industrial IoT is well-understood from widespread deployments over many years. Wi-Fi can be deployed anywhere, globally, in unlicensed spectrum, using a wide range of inexpensive devices and infrastructure. Paradoxically, the ubiquity of Wi-Fi has driven misconceptions: enterprise class WLANs have for many years deployed very strong security and quality of service, but as these features are not activated in residential and coffee-shop hotspots, perceptions that Wi-Fi is insecure, and best-effort persist outside of the networking industry.

Our first 4G model for Industrial IoT involves connecting IoT devices directly to the public cellular network. This has some obvious advantages including ubiquitous network availability and inter-carrier roaming, predictable (but definitely non-zero) connectivity costs and avoidance of private networking costs, and high-rate connections. But there are challenges. Cellular network operators have historically offered a single-class consumer service. While their network equipment is technically capable of providing differentiated quality of service, they do not market such services, so unless they are able to modify their processes and business models, an Industrial IoT customer would not be able to rely on priority of QoS service level agreements for their traffic, allowing cellular network congestion to adversely affect Industrial IoT traffic. Consider, for example, a traffic accident on a freeway where the temporary capacity demand-surge from stationary vehicles could affect a nearby industrial facility. Or a natural disaster like a hurricane where there is huge demand for the network and emergency services traffic is given priority over consumer traffic, but there is no intermediate priority for industrial control traffic. Cellular operators will need to overcome these challenges and more to price and deliver new Industrial IoT services if they wish to make progress in the Industrial IoT market.

The second 4G model is where an organization builds its own private rather than public network, using cellular equipment but in private, licensed spectrum. Customers, in this scenario, would acquire licensed spectrum, purchase cellular equipment and build and operate their network using this, rather than Wi-Fi equipment in unlicensed spectrum. The most attractive aspect of this model is that licensed spectrum is guaranteed to be free from other users, making interference less likely. Depending on the frequency band used, it is also likely to allow higher-power transmissions and have greater range than Wi-Fi, and consequently fewer base stations will be required for a given topology. However, very little licensed spectrum is currently available for private use; only a few countries have such allocations. This is not surprising, given the general spectrum shortage and that cellular operators with their deep pockets acquire substantially all useful spectrum that comes to auction. The options for private organizations to secure licensed spectrum are slim, and even when they are able to, they will need to consider IoT device availability for that band. Apart from the lack of interference, vendors of cellular equipment for this market claim a number of advantages over Wi-Fi, which we will deal with in the next model.

Our third 4G model is for cellular technology deployed in unlicensed spectrum, the same bands at 2.4 GHz and 5 GHz used today by Wi-Fi and also future shared-use bands, notably at 3.5 GHz in the US. At this point, the lower probability of interference in licensed bands no longer differentiates from Wi-Fi, so cellular equipment vendors have begun to extrapolate perceived characteristics of the cellular network to make claims for this model. Some of these claims are technical: spectral efficiency, high data rates, strong QoS, while others are broader and cover reliability and security. As we show with an extensive technical survey in a companion paper, the underlying technologies used in Wi-Fi and cellular standards have a great degree of commonality and will continue to converge in the next-generation architectures used by Wi-Fi 6 and 5G. Depending on assumptions and the particular time interval for comparison, it is possible to claim that either has higher rates, greater spectral efficiency or stronger QoS. That is not to say that Wi-Fi and cellular networks for Industrial IoT in unlicensed spectrum are undifferentiated, but the differences are at the higher layers. Because 4G/5G stems from the current cellular market, it has some limitations in identity and authentication techniques, being SIM-anchored, and brings a complex and expensive network infrastructure requirement that is well-suited for serving millions of cellphones but not flexible for smaller numbers of diverse IoT devices. Meanwhile Wi-Fi has an architecture that evolved in enterprise WLANs and is responsive to enterprise authentication needs, supporting certificate and username/password authentication in addition to SIM authentication for example, along with QoS and strong security options.

How, then, should a large industrial organization choose a wireless technology direction for its IoT architecture? The survey of four network models, above, noted many differentiators, and later in this paper we present a decision-tree, but decision makers should bear in mind the following significant considerations.

First, the underlying waveforms and low-level protocols of Wi-Fi and 4G/5G have much commonality and are converging. The differences in spectral efficiency, data rates, latency, even QoS are not significant enough to drive decision-making. The only significant areas of performance differentiation are that Wi-Fi does not operate effectively when devices are moving at freeway speeds, and 4G/5G can cover longer ranges from the base station, but only if operating in low-bands and at high-power under licensed spectrum regulations.

However, licensed spectrum is fundamentally ‘cleaner’ than unlicensed. The lack of interference from other users (though not from ‘unintentional’ transmitters) makes it inherently easier to build reliable wireless networks. Unfortunately, licensed spectrum is difficult and expensive to procure, precisely because it is scarce and attractive. If an industrial organization could acquire private spectrum in a consistent frequency band across its global properties and satisfy itself that a sufficient variety of IoT devices are band-capable, this would be an attractive option. But these requirements will be unattainable in most cases, and if available will be costly.

Authentication and security are other areas for comparison. Wi-Fi embraces a broad range of security protocols, and the simple-to-configure options used in home networks are quite different from the military-grade protocols deployed in enterprise WLANs for many years. While the strength of authentication and encryption differs little between Wi-Fi and 4G/5G, the variety of identity formats and credentials available on Wi-Fi is much richer than the predominantly SIM-based authentication used by cellular infrastructure.

Many large industrial organizations are currently working on architectural blueprints for IoT systems, as it is well-established that IoT is capable of transforming the way factories, industrial plants and mineral extraction sites operate. These blueprints often focus on how sensors and actuators monitor and control equipment, and the compute and storage capabilities required to consume and draw inferences over that information, and for good reason: these are the essential elements of an IoT system. But the wireless network used to communicate with IoT devices represents an important decision-point, where a lack of attention can limit the functionality of the overall system.

This paper surveys the capabilities and deployment scenarios for Wi-Fi and 4G/5G-based networks for Industrial IoT across four network models. Each model has its strengths and weaknesses, and it is likely that, for the next few years at least, large geographically dispersed Industrial IoT customers will adopt a hybrid approach, using Wi-Fi across most installations while experimenting with 4G/5G architectures for niche requirements and special cases.

TABLE OF CONTENTS

INDUSTRIAL IOT IN A 5G WORLD - ARCHITECTURE 1

ABSTRACT 2

EXECUTIVE SUMMARY 2

INTRODUCTION: INDUSTRIAL IOT 7

WIRELESS TECHNOLOGY CHOICES FOR INDUSTRIAL IOT 8

4G AND 5G TECHNOLOGY AND LICENSED – UNLICENSED SPECTRUM 9

INDUSTRIAL IOT WIRELESS NETWORK MODELS 9

MODEL 1: PUBLIC 4G NETWORKS 9

MODEL 2: PRIVATE 4G NETWORKS IN LICENSED SPECTRUM 12

MODEL 3: PRIVATE 4G/5G NETWORKS IN UNLICENSED SPECTRUM 15

MODEL 4: WI-FI NETWORKS 16

SITE DEPLOYMENT COMPARISONS 19

OFFICE BUILDINGS 19

FACTORY BUILDINGS 20

OUTDOOR PLANT 21

ISOLATED, MULTI-SITE NETWORKS 22

FUTURE DEVELOPMENTS IN CELLULAR TECHNOLOGY FOR INDUSTRIAL IOT: 5G 23

5G NEW RADIO 23

OTHER 5G COMPONENTS 25

NEW DEVELOPMENTS IN WI-FI FOR INDUSTRIAL IOT: WI-FI 6 28

RELIABLE INDUSTRIAL WIRELESS NETWORKS 32

SECURITY 32

CONCLUSION 34

APPENDIX 1: MISSION-CRITICAL SERVICES DECISION TREE 35

INTRODUCTION: INDUSTRIAL IOT

Recent advances in technology have driven extraordinary improvements in the speed and reliability of communications links, the pervasive reach and power of computing and storage, and the business insights gained from data mining and analytics. This revolution is now set to transform the way factories and industrial process plants are operated, through the Internet of Things (IoT).

IoT is broadly defined to include any connected device that is not hand-held by a consumer. In the industrial plant, it embraces existing monitoring, control and telemetry networks and extends to many new sensor and control devices that could eventually lead to full 'lights-out' operation through comprehensive monitoring and control. IoT takes existing systems and transforms them through universal connectivity, miniaturization and reduced cost to collect an exponentially greater variety and volume of data and deliver it to centralized or distributed data-lakes for analysis.

Examples of Industrial IoT include:

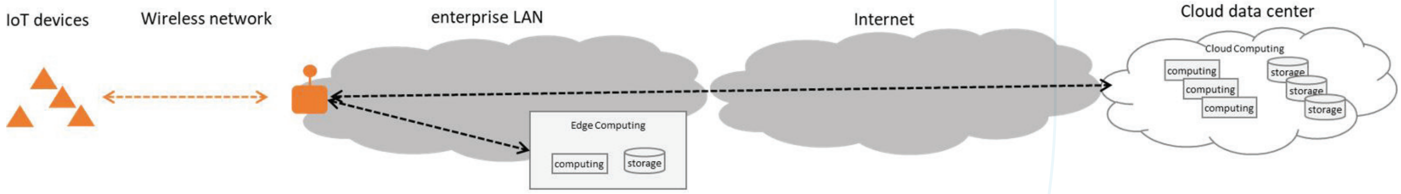
1) Monitoring of pressure, temperature, flow rate and other environmental & process control parameters.

2) Controlling pumps, valves, conveyer belts etc.

3) Imaging items on a conveyer belt to detect flaws, identify alignment, etc.

4) Video sensing as part of a robotic manufacturing cell with automated control loops.

General industrial IoT architecture



5) Compare discrete manufacturing achieved capacity levels to its design targets.

6) Monitoring weld quality and placing orders for consumables for welding operations.

7) Area video surveillance for security or safety purposes.

8) Environmental sensing for quality assurance purposes, ensuring temperature, humidity etc. are within allowed limits.

9) Vibration and condition monitoring, enabling the move from scheduled to predictive/conditioned maintenance.

10) Monitoring wastewater and effluent for purity, to meet regulatory requirements.

11) Monitoring and controlling AGVs (Autonomous Guided Vehicles).

12) Use of AR (augmented reality) goggles to superimpose labels and instructions over images of complex equipment, providing a video assembly & repair manual.

13) Automate material handling systems, including control of warehouse robots.

14) Telepresence for maintenance/service when the technician streams a live, real-time video feed from the device under repair to an expert technician from the vendor of the equipment.

Industrial IoT (or 'Industry 4.0') builds on prior systems such as SCADA, telemetry and industrial control, but differs in scope and scale.

1) Many more sensors report data, ranging from low-rate periodic measurements to high-definition video at rates that were not previously possible.

2) The network (including the wireless part covered in this paper) moves this data to compute and storage nodes in the cloud, central data centers or distributed-coordinated edge compute nodes where it is made accessible through APIs.

3) The power of big-data analytics, machine learning or artificial intelligence operates on the combined data sets to extract patterns, trends and analytics.

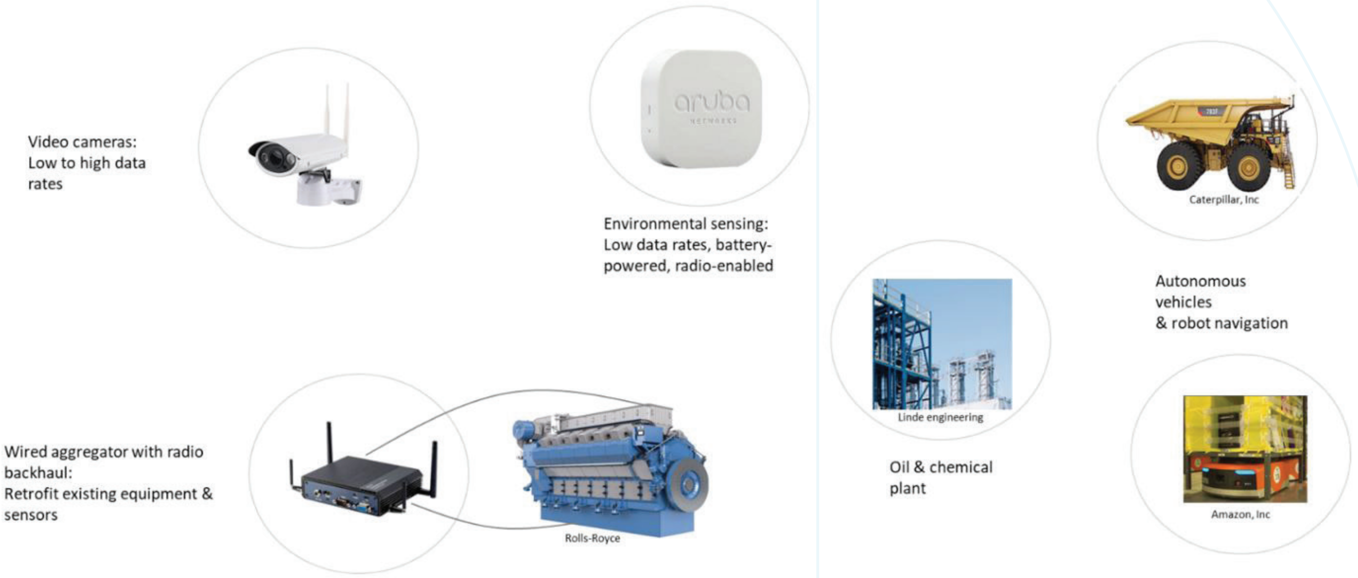
4) Where analysis results in corrections or actions, these control signals are carried back over the network to actuators and controllers.

5) In addition to building focused, individual control systems around dedicated sensors and actuators, Industrial IoT collects orders of magnitude more data from many places in a plant and combines them flexibly under software

control. Once the data-gathering and storage architecture is in place, analysis and control systems can be designed, built and modified without hardware dependencies.

In the short- and medium-term, Industrial IoT will include existing Operational Technology (OT) sensors and many specific protocols such as MODBUS, Bacnet and PROFINET. Next-generation IoT architectures need to embrace these existing systems. Local aggregator equipment is available to interface with existing protocols and sensors. New generations of sensors are already wireless-ready, incorporating radios for individual wireless connections.

Some industrial IoT sensor and connectivity applications



While there is much excitement over the compute and storage implications of the IoT revolution, it is the communications aspects, and specifically the wireless 'last hop' at the edge of the network that concern us in this paper.

WIRELESS TECHNOLOGY CHOICES FOR INDUSTRIAL IOT

The 'last hop' for Industrial IoT is becoming wireless wherever possible, allowing for lower cost, greater flexibility and high mobility. A key question, which we will investigate in this paper, is which wireless technology to select. We will deal in some detail with 4G and 5G cellular networks, since they cover several network models that are not well-understood, comparing their capabilities with Wi-Fi of the 5th and 6th generations. Other technologies, including ZigBee and Bluetooth, may be useful for niche applications but are not suitable for large-scale Industrial IoT networks.

As later sections of this paper will show, even industrial and plant IoT is a broad subject and includes many environments. For example, oilfields can cover significant geographic areas, far from existing cellular coverage and with sparse connectivity requirements; while instrumenting factory equipment may require very high-density, high-speed communications, particularly if real-time imaging is employed; this will also drive latency requirements. Some IoT devices must operate from battery power, imposing limitations, while others are attached to large machines and can be powered locally. Another dimension is reliability: all communications should be reliable, but as applications range from data-gathering to safety-critical processes, appropriate wireless technologies must be selected.

While the wireless technologies of interest for Industrial IoT are broadly 4G/5G and Wi-Fi, many network deployment architectures exist within these technologies. It is important to analyze each model individually, as each has its strengths and weaknesses and the perceived advantages of 4G and the 5G vision are not applicable to every model. There is also growing confusion over what constitutes '5G'. Service providers are already applying the label to 4G networks when it suits their marketing needs, claiming that their performance already meets some 5G metrics. Similarly, some technologies required for 5G, such as indoor small cells, have been marketed for many years with limited success, and service providers hope that applying the 5G label in combination with other 5G capabilities will provide the impetus necessary for commercial success. In the remainder of this paper, we deal in detail with '4G' technologies, broadly available today but with varying levels of market penetration, and distinguish these from '5G' which is still predominantly standards and slideware and will progress to products and services for the Industrial IoT market over the 2020 – 2025 time period.

4G AND 5G TECHNOLOGY AND LICENSED – UNLICENSED SPECTRUM

The 5G vision, expressed in standards from the 3GPP (3rd Generation Partnership Project) standards development organization, follows 2G, 3G and 4G in sequence but is much broader in scope. Whereas, up to 4G, the standards were aimed at building a better cellular network - as we know mobile networks today - 5G standards include new technologies that will allow service providers to move beyond familiar voice-text-and-Internet-to-cellphones services to enter new markets, should they wish to do so.

5G standards provide the technology for mobile operators to move into new markets including broadband-to-the-home over fixed wireless links, enterprise networks with indoor small-cell radio units, wide-area, low-bandwidth connections for IoT, and industrial networking in factories and production plants with low-latency, high-reliability connections to industrial robots, process control and monitoring equipment.

The initial set of 5G standards is complete, but commercial deployments will be phased over a period of several years. As of early 2019, initial 5G networks consist of small-scale trials of broadband-to-the-home services and mobile hotspot devices, with limited millimeter-wave radio coverage in some city centers. Upgrades of the 4G network to 5G for mobile consumer use will start rolling out later in 2019 and further market developments will be determined by service providers' organizational and business plans, as they determine whether they are well-placed to reach into the new areas that 5G technology allows them to enter.

A large part of this paper will explore the implications of 5G technology for enterprises, either as an extension of a mobile operator's network or a standalone private network, as this is one of the new markets targeted by 4G and 5G equipment manufacturers.

While large-scale commercial 5G deployments are in the future, some vendors of 4G equipment are exploring new markets, outside public cellular networks, including the emerging Industrial IoT market. The proposed architecture is, broadly, to shrink a cellular operator's network to fit a single industrial plant's needs. This 'private LTE' concept (we will use the terms 'LTE' and '4G' interchangeably in this paper) comes in a variety of network models, including CBRS, MulteFire (for licensed and unlicensed spectrum) and in 4G and 5G variants. It is distinct from the mobile operator's 4G or 5G network described above, and is in many ways the equivalent of today's Wi-Fi WLAN, but using cellular radio technology and associated 3GPP core network elements and protocols. This approach has some attractive aspects, but even with the small number of current deployments, limitations are becoming apparent.

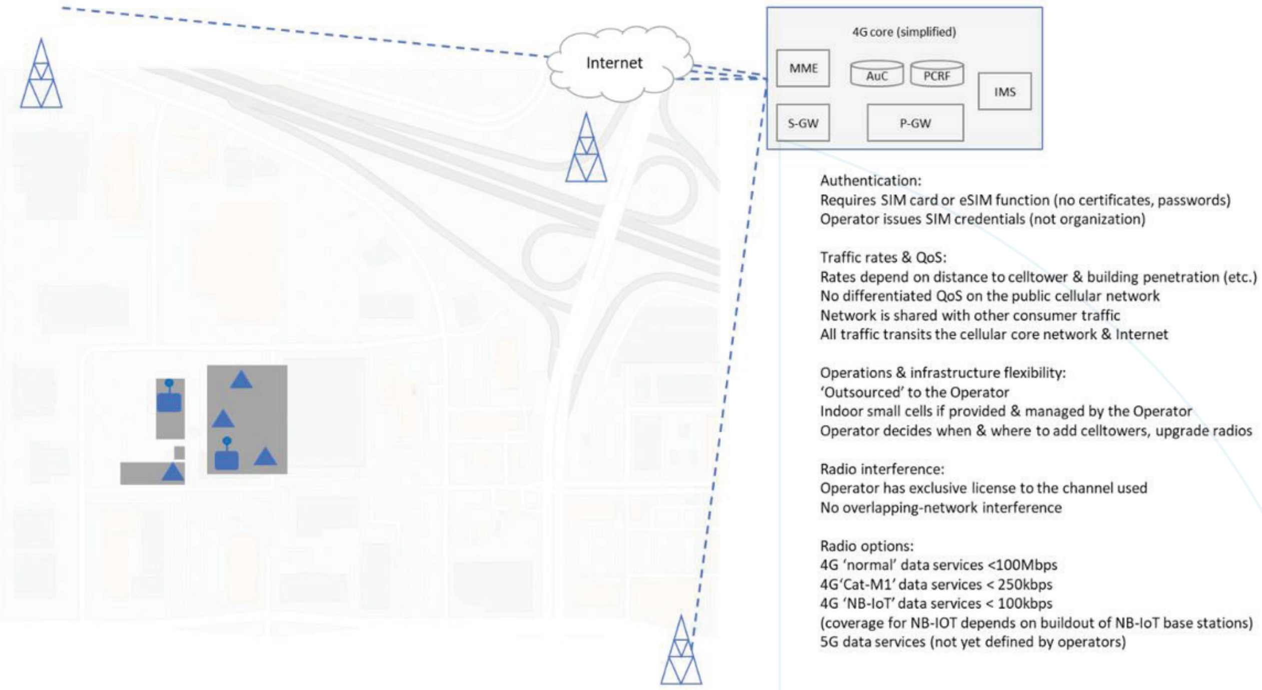
INDUSTRIAL IOT WIRELESS NETWORK MODELS

This paper will consider four network deployment models. Each comes with variations, which we will also explore. The characteristics of these primary models will be significant drivers of the behavior and performance of an industrial customer's IoT system.

MODEL 1: PUBLIC 4G NETWORKS

In this model, the mobile operators that run the public cellular system extend their network inside enterprise campuses and factory buildings. Some customization and partitioning for improved service is possible, but customers always connect IoT devices directly to the operator's network, in the same way as a cellphone would connect to the public cellular network today. One benefit of this model is that, as an extension of the cellular network, existing subscribers with cellphones and other devices will be able to connect. It is a way of extending cellular coverage, provided the mobile operator is prepared to install new base stations where required.

Model 1: IoT on the public cellular network



Authentication:
Requires SIM card or eSIM function (no certificates, passwords)
Operator issues SIM credentials (not organization)

Traffic rates & QoS:
Rates depend on distance to celltower & building penetration (etc.)
No differentiated QoS on the public cellular network
Network is shared with other consumer traffic
All traffic transits the cellular core network & Internet

Operations & infrastructure flexibility:
'Outsourced' to the Operator
Indoor small cells if provided & managed by the Operator
Operator decides when & where to add celltowers, upgrade radios

Radio interference:
Operator has exclusive license to the channel used
No overlapping-network interference

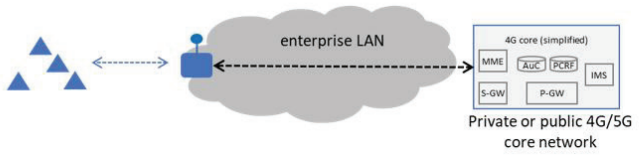
Radio options:
4G 'normal' data services <100Mbps
4G'Cat-M1' data services < 250kbps
4G 'NB-IoT' data services < 100kbps
(coverage for NB-IOT depends on buildout of NB-IoT base stations)
5G data services (not yet defined by operators)

As cellular operators started to investigate various markets beyond the consumer, including Industrial IoT, they encountered challenges with the topology of their current network. On too many enterprise premises, coverage is inadequate either in terms of signal strength for high-rate connections, or for the high-capacity requirements of enterprise customers. Since it is both costly and cumbersome to add cell towers and macro base stations, operators have resisted such buildouts for specific enterprise customers, and have looked instead to install 'small cell' radios inside the enterprise.

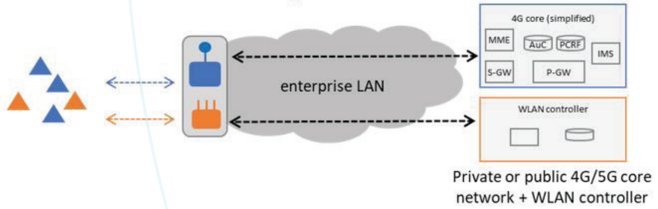
Where signals cannot penetrate a building, or the nearest cell tower is too distant to give a good indoor signal, operators can extend coverage by adding small cells to their networks.

Small cell equipment has existed, in some form, for over 20 years. Its goal is to shrink a standard cellular base-station or radio unit so it can be wall-mounted indoors, like a Wi-Fi access point. As they use cellular frequencies and power levels, fewer small cells are needed to cover a given indoor area than for the equivalent Wi-Fi WLAN, perhaps 3x or 4x fewer units, but it has proven very difficult for equipment manufacturers to reach price points where they can compete with Wi-Fi for a given level of coverage.

Single technology 4G/5G small cell



Combined technology 4G/5G + Wi-Fi small cell



The technology has other potential advantages: small cells can directly support consumer cellular devices in addition to IoT sensors, providing indoor coverage in hard-to-reach areas. But the current 4G small cells have revealed several significant obstacles to deployment:

1) Multi-operator support is limited. While several architectures exist to allow a single small-cell to serve subscribers of other operators, small cell deployments remain – in practice – single-operator.

2) Management is an issue. The mobile operator is responsible for compliance with spectrum licensing rules, and will require direct control and management of the small cell transmitters. But, as these radios rely on enterprise LAN and WAN connectivity to reach the mobile core network, there is an uneasy delineation of management responsibilities. For example, will the enterprise be allowed to move a small cell to a new location, or will the operator's technician be required? How does the enterprise ensure its LAN bandwidth is not overwhelmed by small cell traffic, while the operator ensures its traffic gets sufficient priority to meet its service-level requirements? These issues are not easy to solve in practical networks.

3) Which users are supported? Typically, an enterprise or public-facing venue will want its own employees' traffic to get priority over members of the public passing-by. But this is difficult to achieve – how should the enterprise identify its users' devices and convey this information to the mobile operator, which traditionally runs a consumer-grade network with one class of service? This raises a related issue: authentication relies on the service-provider's infrastructure and every new device on the network needs a SIM card and subscription, a cumbersome as well as potentially expensive requirement.

4) How to accommodate existing Wi-Fi devices, especially Wi-Fi-only devices? Enterprises have many of these, often 'legacy' devices that cannot be easily upgraded; the installed base is large, and cellular small cells cannot support it. The usual solution is to incorporate a Wi-Fi network alongside the small-cell network, but this adds to the expense, and the two networks are not integrated on the user-plane, control-plane or management-plane. Most service providers do not wish to manage an enterprise Wi-Fi network (although exceptions are emerging in service provider managed Wi-Fi, these providers are usually separate organizations from the mobile network operations team).

5) Cellular technology is not inherently backwards-compatible. While a current-generation Wi-Fi access point can serve any Wi-Fi device ever produced, cellular radios are single-technology. Similarly, a Wi-Fi 6 client will connect to a Wi-Fi 5 access point (with Wi-Fi 5 features), but a 4G small cell cannot serve 3G or 2G clients. Therefore, organizations must choose a generation or snapshot of 4G/5G radio technology and are constrained in the range of clients that can connect. Today, the pressing decision is whether to purchase and install 4G small cells, knowing they can serve current 4G sensors and devices, or to reach for 5G and accept a much more limited range of clients.

6) A further consideration is the ability and willingness of mobile operators to customize their network to the needs of enterprise and industrial customers. If the locations to be used already have good, high-capacity cellular coverage there is unlikely to be a problem; but if even a few outlying factory locations are not well-covered, the customer will need to approach its cellular provider to install new base-station radios or other equipment. Experience to date shows mobile operators have not been over-flexible in this regard, when dealing with complaints of poor enterprise coverage. This may change, but it needs to be considered in planning, as does the ability and willingness of the chosen mobile operator to support roaming onto other cellular providers' networks when a sensor may move to a new location. While roaming is technically supported over cellular networks, it may not be a specific feature of a given mobile operator's SIMs, and roaming behavior in the cellular network is – for now – a matter of operator policy.

7) Perhaps the most significant barrier for small cell deployments has been the limited business case for operators. At present, these service providers are optimized to manage spectrum, build and maintain the macro public cellular network, and market their services to consumers. It would require very significant changes to their planning, installation, commissioning, network management and help-desk functions to move into the managed-enterprise-network market with small cells, and – thus far – mobile operators have not been able to make compelling business cases for transforming their organizations in this way.

Small cells, while quite widely-used to augment residential coverage (as 'femto-cells') and in the macro public cellular network, have to date failed to penetrate the enterprise, due to a number of shortcomings of which the weak business case and required changes to the operator's organizational structure are the most significant.

The 5G architecture adds a number of building-blocks beyond small cells that make it more attractive for enterprise and Industrial IoT networking. We cover these in the 5G section of this paper.

Apart from small cells, many IoT-friendly features already exist in today's 4G standards but, while the technology and equipment already exist, mobile operators have not yet moved into major differentiated enterprise markets such as in-building deployments of small cells or Industrial IoT on the 4G network.

Perhaps the most developed operator IoT market today is connected-cars, utilizing standard LTE connections for the most part, although low-rate enhancements like NB-IoT and LTE Cat-M1 – low-rate connections that can be marketed at lower price points – are beginning to roll out for wide-area coverage roles. These are already useful. IoT sensors or OT sensor aggregators fitted with 4G radios can be expected to work anywhere in the country, and with roaming agreements world-wide. This wide-area coverage of the cellular network is critical to vehicle-borne sensors but may not be applicable to buildings, factories or process-plants.

Aside from the niche IoT applications available today, most operators are waiting for the many new features that will be available with the 5G architecture, which will better equip them to enter new markets including Industrial IoT with standard 5G features. The speed of the 5G upgrade cycle and proliferation of new services will depend on the incremental revenue and reduced costs that operators can realize from 5G. Most analysts predict that 5G connections in the public network will not pass 50% of the total until 2025 or later.

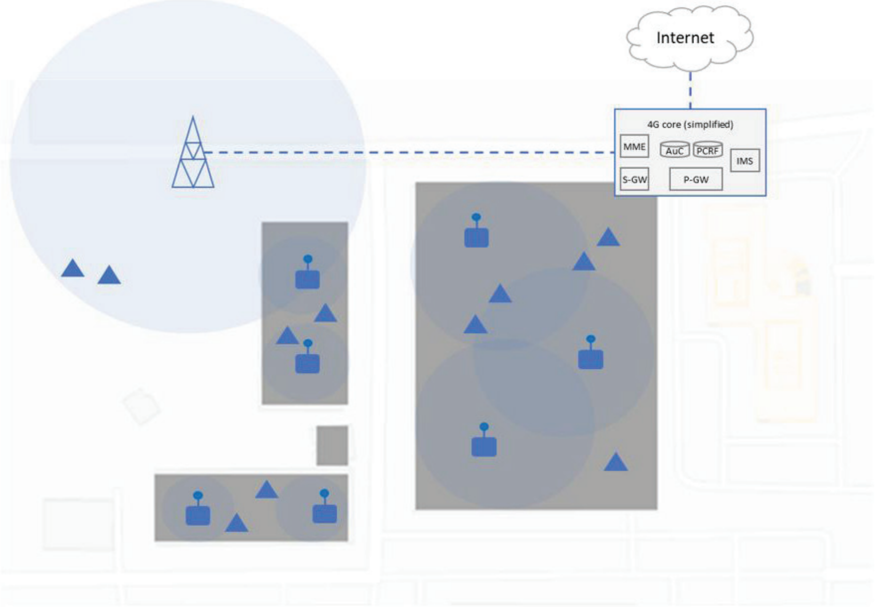
Apart from ubiquitous wide-area coverage, the second important property of cellular technology is its ability to support high-speed mobility. Where devices move at greater than 70 km/hr, cellular connections work better than Wi-Fi. But this use-case covers limited applications.

As we will show later, if universal wide-area coverage and high-speed mobility are not required, extending the cellular network for IoT may not be the preferred solution. For instance, Wi-Fi is a more flexible edge radio, and can be used with local aggregation technology and backhaul over the cellular network, for reduced costs and more flexibility in sensor selection and configuration. Alternatively, for wide-area coverage, a combination of Wi-Fi point-to-point links, mesh networking and local access may be easier to deploy and manage than a hybrid with the public cellular network.

MODEL 2: PRIVATE 4G NETWORKS IN LICENSED SPECTRUM

It is possible to take 4G equipment originally developed for large-scale public cellular networks, and re-purpose it for private networks that can be built for individual organizations. Depending on the networking equipment vendor, network topologies will be offered in a number of variants. Although extended specifications exist, these networks will, for the short- and medium-term, be islands of connectivity, separate from public cellular systems. They will be connected to the Internet but unable to authenticate public cellular devices or allow phone calls across the public network. In this sense they are closer in capability to today's Wi-Fi networks than cellular networks.

Model 2: IoT on a private 4G network (licensed spectrum)



Authentication:
Requires SIM card or eSIM function (no certificates, passwords)
Organization issues SIM credentials
No roaming to the public cellular network

Traffic rates & QoS:
Rates depend on infrastructure limits & radio placement
QoS is possible if supported by infrastructure

Operations & infrastructure flexibility:
Organization owns and operates core network and radios
Organization decides when & where to add, upgrade radios
Outdoor celltower & indoor small cell radio options

Radio interference:
Organization has exclusive license to the channel used
No overlapping-network interference

Radio options:
Requires sensor radios capable of the allocated licensed band
4G 'normal' data services <100Mbps
4G'Cat-M1' data services < 250kbps
4G 'NB-IoT' data services < 100kbps
(NB-IOT depends on availability of NB-IoT base stations)

The previous section explored the network model where a mobile operator extends its public network into an enterprise or industrial facility. This would be attractive where the chosen operator already provides satisfactory coverage in all required locations and areas, and where the lack of control and strong service-level guarantees is not a significant drawback. But most operators have not yet customized their networks for industrial customers, and many factory and process plant operators are not ready to make such a decision.

For this case where licensed frequencies are used, building a network involves the company obtaining a license to use a particular frequency, then building a dedicated network offering service in that channel, and connecting IoT devices.

Licensed, private spectrum – one of the strongest arguments in favor of building Industrial IoT networks on 4G/5G equipment – is an attractive concept because it can ensure absence of interference. The spectrum owner is assured that no other transmitters can operate in this spectrum. There is complete control over the devices authorized to access the network, and customization and tuning such as defining and assigning class-of-service priorities is under the control of the network owner.

To build a private 4G network on private spectrum, an organization must first obtain frequencies that no one else can use in the target location, then adapt equipment built for 4G network infrastructure to operate on these frequencies, and of course source IoT devices capable of using these frequencies.

But the first requirement, spectrum availability, can present a very significant obstacle.

1) While the concept of private spectrum for coverage (rather than narrowband point-to-point) networks has existed for many years, very few networks using private spectrum exist today, and they tend to be special cases - for example oil platforms and mines that are geographically isolated from population centers and cellular networks, or a handful of countries world-wide that have experimented with liberalized licensing regimes. This means that, while the concept of private spectrum exists, the practical obstacles to obtaining such spectrum (as well as the costs, if spectrum becomes available) are significant, to the extent that while such networks have been possible for decades, very few exist today.

2) An alternative to obtaining spectrum direct from the national regulator would be to sub-lease from an existing cellular or mobile operator, as these organizations have extensive spectrum holdings. Again, very few practical examples exist today, as national regulations often discourage sub-leasing of spectrum, and, since it is a scarce and costly resource, operators already use, or expect to use the balance of their allocation.

3) As private spectrum is difficult and expensive to acquire, often the only practical way a private organization can access licensed spectrum is to work closely with an existing mobile operator. This model has been seen for some years with indoor small-cells, and it involves sub-contracting or outsourcing installation and management of the network to the mobile operator, as the operator wishes to control the particular channels used by the network, often to avoid interference with adjacent public services, and to ensure it complies with the legal requirements of the spectrum license. In the limit, it becomes our Model 1 above. The benefits for the plant owner are that the costs of leasing spectrum and operating the network are borne by the mobile operator (although they may be passed on in commercial contracts). But outsourcing relationships require considerable management, and few offer the control and flexibility that accrues from organically managing a private network.

As noted above, private spectrum allows a plant owner to exercise control over all aspects of the network, while taking on the costs of leasing the spectrum, and building, operating and maintaining the network, supporting it with organic or sub-contracted expertise. The control aspects often make it the preferred model, but constraints of cost and availability usually direct plant owners to compromise, through a cooperative arrangement with a mobile operator.

Assuming access to licensed spectrum is assured, the industrial customer is ready to build a network. The only infrastructure equipment available for this spectrum will be that used in the public cellular network, or variations, and while this is often presented as an advantage, the needs of private networks differ substantially from the mobile operators.

1) Consider scale. Mobile operators work with millions of subscribers, and thousands of simultaneous connections across a town. Standards and equipment are designed with this in mind. This results in high complexity and high cost-points. While private 4G equipment designers have spent many years shrinking cellular equipment down to private networking dimensions, it still carries a substantial price premium.

2) But price is not the most significant issue. 3GPP standards are focused on the needs of the public cellular network, lacking the flexibility familiar to private network managers. For example, authentication on cellular networks relies on specific protocols, linked to SIM cards in the client device. Client selection is limited to devices that incorporate 4G radios and support SIM cards. Today, that is a much more limited list than for Wi-Fi, which supports authentication options including passwords, X.509 certificates as well as SIM cards (through EAP-SIM/AKA/AKA'). The owner of a private 4G network will have to program their own SIM cards and support an AAA server to authenticate them, and will be unable to support non-SIM clients.

3) In addition to managing SIM authentication infrastructure, the network manager will need to become familiar with other aspects of cellular technology, including network operations and management, and RF planning.

4) All these issues can be managed, but they add friction for network engineers facing the task of building and managing a private 4G network.

5) All of the new features introduced as 5G supersedes 4G will be applicable to private networking. If private 4G networks in private spectrum gain significant market share, expect to see 5G enhancements like MEC instances and Network Slicing (discussed later in this paper) added to the architecture to give the same benefits as for the public cellular network extended for enterprise use.

6) Equipment and device backwards-compatibility. The radios of a private 4G/5G system will be built for a single 3GPP technology: 3G (still available), 4G (several variants available from LTE to LTE-A and LTE-A Pro) and then 5G. Unlike Wi-Fi, the public cellular network has no tradition of backwards-compatibility in its equipment (although the overall network can support different generations, this is through overlapping coverage from different infrastructure). This means that today's 4G base stations will not support forthcoming 5G clients, and vice versa. The choice of technology to purchase will lock-in performance and client compatibility for the lifetime of the network.

7) 4G equipment vendors make other arguments for using their equipment in private networks. Many of these arguments suggest 4G-LTE and 5G are superior to other options such as Wi-Fi due to the radio technology. As explained in our companion paper on technology, radio waveforms used by 4G/5G and Wi-Fi are similar and converging: there is no sustained advantage of one over the other. The benefits of a private 4G/5G network over Wi-Fi are:

a) Limited interference. Frequencies are allocated to the user organization for its exclusive use. This prevents 'intentional transmitters' from using the frequencies, but it does not, of course prevent unintentional electro-magnetic interference. And, in exchange for this interference-free guarantee, the spectrum license will be expensive: all such spectrum is auctioned by government regulators to raise revenue.

b) The range of a radio link. This is due to licensed spectrum being at lower frequencies than Wi-Fi spectrum, and licensing rules that allow higher transmit power in most licensed bands. The result is that, in most cases, fewer base station sites are required for 4G/5G over Wi-Fi.

c) The breadth of geographic coverage, country-wide and international. While this is a real benefit where the public cellular network is used for Industrial IoT, it is not true of private 4G/5G networks. Roaming-in of public network subscribers, and roaming-out of devices to the public network is not supported by today's implementations, even though standards models exist.

d) High-speed mobility. Where devices move in excess of 70 km/hr, a 4G/5G solution is applicable.

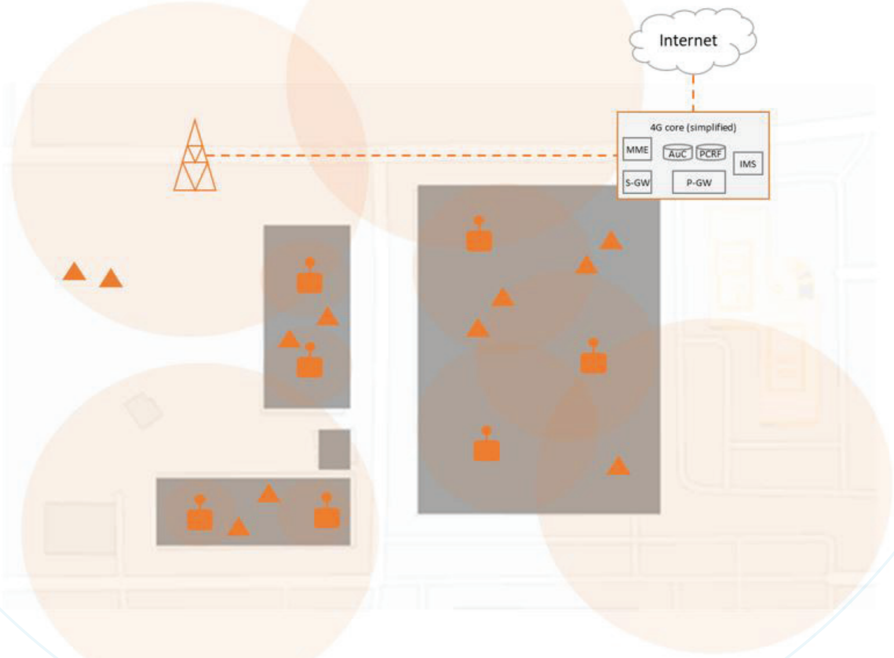
With our 4-way classification of Industrial IoT network models, the CBRS system fits here as private 4G/5G networking, as the spectrum is licensed, and the equipment is derived from 4G/5G standards. But there are a number of caveats to the CBRS story:

Across the most populated, coastal areas of the country, there is no guarantee of spectrum availability. CBRS defines three tiers of spectrum-user, in a hierarchy where the less-important is pre-empted by higher tiers. As currently defined, the highest tier is reserved for incumbents, primarily government users of which a significant number are ship-borne radars. This means that any private CBRS licensee within 50 miles of the coastline can be pre-empted by maritime traffic, and forced to cease transmitting. And it is not clear whether, when CBRS spectrum auctions open, mobile operators and other large service providers will quickly lock up the majority for internal use, leaving little for private organizations. Much remains unclear, and will remain so into 2020.

CBRS uses new spectrum, not previously available in the USA. This means that, although some devices and network equipment exist with this operating frequency, they will be built specifically for the CBRS experiment or available for the Japanese market, the one area that uses this band for public cellular service. It is currently unclear whether mainstream North American cellular devices will support the CBRS bands, so the range of available client devices may be limited.

MODEL 3: PRIVATE 4G/5G NETWORKS IN UNLICENSED SPECTRUM

Model 3: IoT on a private 4G network (unlicensed/shared spectrum)



Authentication:
Requires SIM card or eSIM function (no certificates, passwords)
Organization issues SIM credentials
No roaming to the public cellular network

Traffic rates & QoS:
Rates depend on infrastructure limits & radio placement
QoS is possible if supported by infrastructure

Operations & infrastructure flexibility:
Organization owns and operates core network and radios
Organization decides when & where to add, upgrade radios
Outdoor celltower & indoor small cell radio options

Radio interference:
Possible overlapping network interference, depending on geography, spectrum band rules & neighbors

Radio options:
Requires sensor radios capable of the allocated unlicensed band
4G 'normal' data services <100Mbps
4G'Cat-M1' data services < 250kbps
4G 'NB-IoT' data services < 100kbps
(all depend on availability of CBRS or MulteFire or eLAA equipment & infrastructure radios)

An industry consortium, the MulteFire Alliance, has developed a protocol where the 4G LTE (Long-Term Evolution) waveform can run in unlicensed bands, primarily the 5 GHz band used today by Wi-Fi. MulteFire has the potential to be used for private or service-provider networking and is likely to be a short-term, pre-standard solution until the 3GPP completes appropriate standards, but to date it has been used more as a forum for examining network architecture than developing commercial products: the MulteFire Alliance is not structured as a standards development organization. In the 3GPP 4G/5G standards model, three protocols allow extension of a network into unlicensed spectrum using 3GPP modulation:

1) LAA (Licensed Assisted Access) is a hybrid solution where a network built on licensed spectrum can use channel aggregation to add downlink-only service in the 5 GHz unlicensed band. LAA is already rolling out in the public cellular network for traffic offload in congested areas such as city centers, but because it relies on an 'anchor' connection in licensed spectrum, it is not capable of building a standalone unlicensed network.

2) A new standard, eLAA (enhanced LAA) will extend the model allow uplink as well as downlink traffic in the unlicensed band but retain the requirement for an anchor connection in a licensed band.

3) A future 3GPP r16 standard, 'standalone NR-U' (new radio in unlicensed bands) will remove the requirement for an anchor connection in licensed spectrum. NR-U will be equivalent to the MulteFire consortium's protocols, but fully standardized by the 3GPP. A future NR-U private network would be architecturally similar to today's Wi-Fi networks.

These technologies have some common characteristics.

1) All use 4G/5G waveforms and core network architectures to build private networks using shrunk cellular infrastructure equipment.

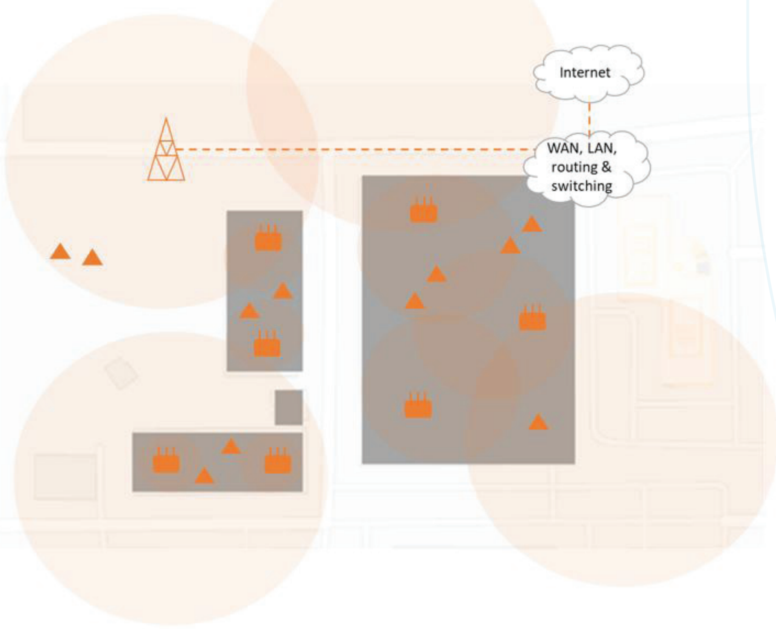
2) This has the same strengths and weaknesses, listed above, as private 4G/5G networks in licensed spectrum, but without the freedom from interference claimed for licensed spectrum.

3) While LAA pioneered the use of LBT (listen before talk) in 3GPP, commercial implementations do not incorporate the same parameters or values as Wi-Fi. Thus, it has not been possible to measure the impact of LAA transmissions on overlapping or adjacent Wi-Fi networks, and vice-versa. This is currently an area of concern to the Wi-Fi vendor and operator community.

4) If networks of this type are rolled out in quantity, it will be interesting to see whether the 4G/5G MAC (Medium Access Control) layer reacts to the presence of other transmitters and overlapping cells as robustly as Wi-Fi, where the protocol was designed from the beginning for these conditions.

MODEL 4: WI-FI NETWORKS

Model 4: IoT on a private Wi-Fi network (unlicensed spectrum)



Authentication:
Can use passwords, certificates (or SIM cards)
Organization issues credentials
No roaming to the public cellular network

Traffic rates & QoS:
Rates depend on infrastructure limits & radio placement
QoS supported across LAN & WAN

Operations & infrastructure flexibility:
Organization owns and operates LAN & access points
Organization decides when & where to add, upgrade access points
Outdoor & indoor access point options

Radio interference:
Possible overlapping Wi-Fi network interference, depending on geography & neighbors

Radio options:
Requires sensor radios capable of Wi-Fi
Rates to > 1Gbps
Depending on distance, number of antennas, etc.

Wi-Fi has been applied to enterprise networks for many years, but the Industrial IoT market is too young for a full understanding of Wi-Fi's capabilities in this context to have developed. The list below includes both widely accepted and less-understood aspects of Wi-Fi for factories and process plants.

The use of unlicensed spectrum means that any end-user can set up or extend a Wi-Fi network, anywhere. This offers an immediate measure of control over any system where spectrum licenses restrict the locations, frequencies and power levels of transmitters.

Similarly, devices can be authorized for network access using the same AAA and directory structures used today by enterprises, based on passwords, X.509 certificates or SIM card credentials. This allows a Wi-Fi network to support a wide diversity of device types and capabilities.

Unlike the cellular network, Wi-Fi can be configured with different levels of security. Increased security usually brings complexity and restricts options, so, for instance, home networks are often open or use pre-shared keys. Enterprise networks should use WPA2-enterprise, a protocol using the 802.1X framework, which provides high levels of authentication and encryption. WPA2-enterprise comes with many options, some of which are accepted for secure and secret government and military networks.

While Wi-Fi is – like any wireless technology – susceptible to interference, it was designed from the beginning to be robust in the presence of other transmitters, intentional or unintentional. The Wi-Fi packet-by-packet MAC design is well-suited for re-transmissions to overcome lost or errored packets.

Like all wireless networks, a large-scale Wi-Fi installation must be well-designed from the RF perspective. The selection of RF channels, transmit power, directional or omni antennas and the placement of access points all affect coverage and signal levels. The same issues will apply to 4G/5G technology when deployed in similar indoor areas. While WLAN vendors have for many years offered software-automated tools for RF tuning in enterprise settings, the industrial environment will offer opportunities to improve these tools.

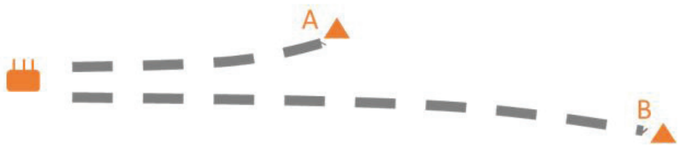
Wi-Fi has a history of backwards-compatibility for its entire lifetime. Access points installed today can support clients built over the last 20 years, and new clients that will be marketed in 2020 and beyond will be able to connect to current Wi-Fi infrastructure.

Coverage of large open spaces using Wi-Fi generally requires more transmitter sites than the equivalent using 4G/5G technology in licensed spectrum. But the simplicity and control available with unlicensed deployment and the lower cost of Wi-Fi equipment will often compensate for the larger number of sites. Point-to-point and mesh Wi-Fi links have been used for many years to extend networks over large campuses and open areas. Wi-Fi only becomes infeasible where distances are very large, or transmitter sites are unavailable.

The current Wi-Fi standard, known as 802.11ac or Wi-Fi 5, has speeds from 6 Mbps to 1.3 Gbps and more. It is being superseded as of late 2018 with 802.11ax, known as Wi-Fi 6, which includes many improvements of interest to Industrial IoT users. Wi-Fi 6 brings important new features (discussed in more detail later in this paper):

1) Orthogonal Frequency Division Multiple-Access (OFDMA) is a multi-user mode where several devices can communicate in the same time interval. It is a technique that has been used in other systems, like cellular-LTE, for many years, and is one of several areas where Wi-Fi and 4G/5G are converging in both technology and features. OFDMA divides a transmission across the frequency dimension, with pairs of devices assigned to transmit and receive in sub-channels where the smallest unit of allocated bandwidth is around 2 MHz. This allows a single access point to serve orders of magnitude more client devices than before, a critical requirement for IoT.

Controlling data-rates and error-rates with OFDMA



Longer range usually means higher RF loss. Adjusting data-rate allows error-rate to be limited.
Example:

- A: range 10 meters, data-rate 172 Mbps -> bit error-rate 0.01%
- B: range 25 meters, data-rate 51 Mbps -> bit error-rate 0.01%...
- ...or B: range 25 meters, data-rate 172 Mbps -> bit error-rate 0.1%

(AP assigns data-rates for both uplink and downlink)

2) OFDMA also enables strong QoS. Prior to this release, Wi-Fi defined 4 levels of priority for different QoS requirements, by specifying timing parameters that ensured higher-priority traffic was able to gain transmit opportunities ahead of lower-priority traffic, as part of Wi-Fi's packet-by-packet MAC structure. OFDMA allows the access point to control medium access for both uplink and downlink, eliminating the need for medium contention, and further, allows the access point to schedule transmissions. This flexible control mechanism enables each client device to be allocated guaranteed bandwidth over the air.

3) OFDMA is also used to reduce latency to arbitrary levels. Whereas previous generations of Wi-Fi only allowed one packet on the air at a time (a few more with MIMO), so a long packet could block traffic, delaying it, OFDMA allows latency-and jitter-sensitive traffic to be allocated frequent, short transmission opportunities so it is never delayed by other traffic in the system.

4) Various improvements extend range, especially for low-rate traffic, by a factor of 2x for a given rate.

5) A new power-save protocol allows devices like IoT sensors which transmit infrequently to sleep for extended periods, saving power and enabling a new generation of battery-powered Wi-Fi sensors.

6) Special attention has been paid to situations where access point signals overlap, driving reduced interference and higher throughput in dense deployments of access points.

7) Data rates have been increased by reducing per-packet overhead and adding new modulation levels.

In summary, Wi-Fi 6 brings the following improvements over Wi-Fi 5:

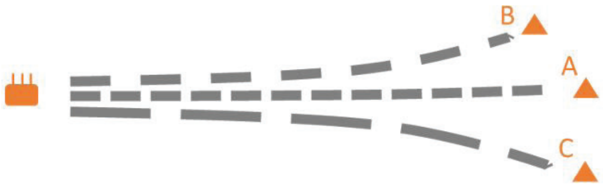
1) Improved QoS, including high- and low-rate clients and scheduled transmission for low latency

2) Support for thousands of clients per access point

3) Stronger QoS and scheduled transmissions

4) Extended battery life

Controlling latency with OFDMA



For the same data-rate, the AP can control latency by assigning transmit opportunities.
Example:

- A: Tx opportunity every 10 msec: 10 msec max latency
- B: Tx opportunity every 20 msec: 20 msec max latency
- C: Tx opportunity every 30 msec: 30 msec max latency

(AP assigns transmit opportunities for both uplink and downlink)

SITE DEPLOYMENT COMPARISONS

It can be difficult to extrapolate from technology and capabilities to practical network design. This section considers a number of sites encountered in Industrial IoT and discusses how they can be served by different technologies.

Office buildings

First, an office building. These are well-understood environments for Wi-Fi WLANs, and current guidelines call for an access point installed every ~15-25 m, with Ethernet wiring to closet LAN switches and either local AC or power-over-Ethernet powering. Due to the increased over-the-air data rates, many enterprise customers are moving from Gigabit Ethernet to multi-Gigabit technology for the AP backhaul. This network design gives extremely high data rates and network capacity: close to 1 Gbps for current production cellphones, and several Gbps per AP. The close spacing allows for > 4,000 Gbps per km^2.

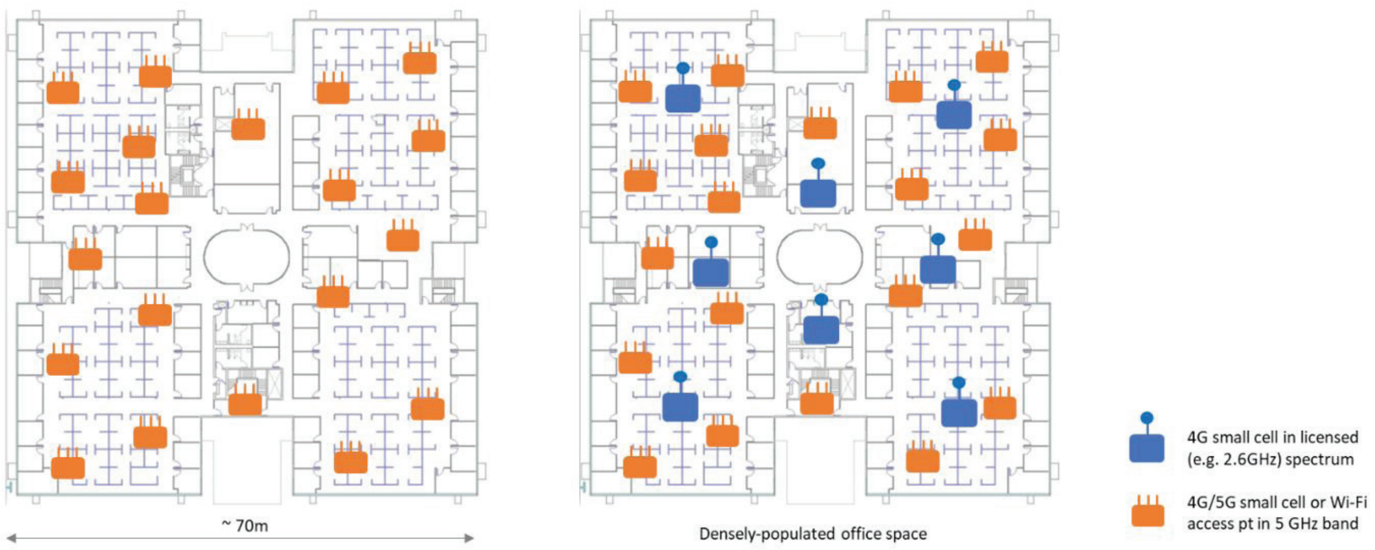
4G small cells have not yet been seen in the enterprise widely enough to gain accurate information, but extrapolation from specifications and small-scale installations indicates that, for mid-band deployments around 2-4 GHz, a coverage area of ~600-1000 m2 can be expected. However, this comes at a much lower network capacity; 4G small cells are generally limited to ~150 Mbps downlink and ~70 Mbps uplink speeds in practice. With a per-cell capacity of ~250 Mbps, overall network capacity will be 250 Gbps per km2, an order of magnitude less than for a Wi-Fi WLAN. It is difficult to increase this figure, because of the limited spectrum available for small-cell deployments. Whereas Wi-Fi can use the whole ~1 GHz of the 5 GHz band across 20+ channels, licensed spectrum is usually available only in 5, 10 or 20 MHz channels.

If high-density and network capacity are not significant goals, Wi-Fi APs can be more widely spaced but this is not often a design choice for enterprise networking in 'carpeted office' spaces.

The resulting networks can be compared: Wi-Fi has superior data rates and far superior network capacity, but requires more access points to cover a given area than 4G small cells. Wi-Fi networks are nearly always less costly than the equivalent small cells, due to the inherent cost and complexity of cellular technology.

Radio placement and coverage on an office-building floorplan

4G small cells operating in 2.6 GHz band under FCC rules cover ~3-4x the area (~900 m^2) of a Wi-Fi access point operating in 5 GHz band (~250 m^2)
If high capacity (> 1 Gbps/AP) is not required, Wi-Fi can be installed at ~500 m^2 per access point.


~ 70m
Densely-populated office space
4G small cell in licensed (e.g. 2.6GHz) spectrum
4G/5G small cell or Wi-Fi access pt in 5 GHz band

Factory buildings

Many Industrial IoT networks serve factories, warehouses and other large buildings. We can identify several choices for serving these buildings.

The outdoor-in scenario has sensors and aggregator routers with 4G modules, connecting to the public cellular network. This is a simple and flexible arrangement, provided the cellular operator can cover the indoor areas with sufficient signal strength and network capacity. No on-site networking equipment is required.

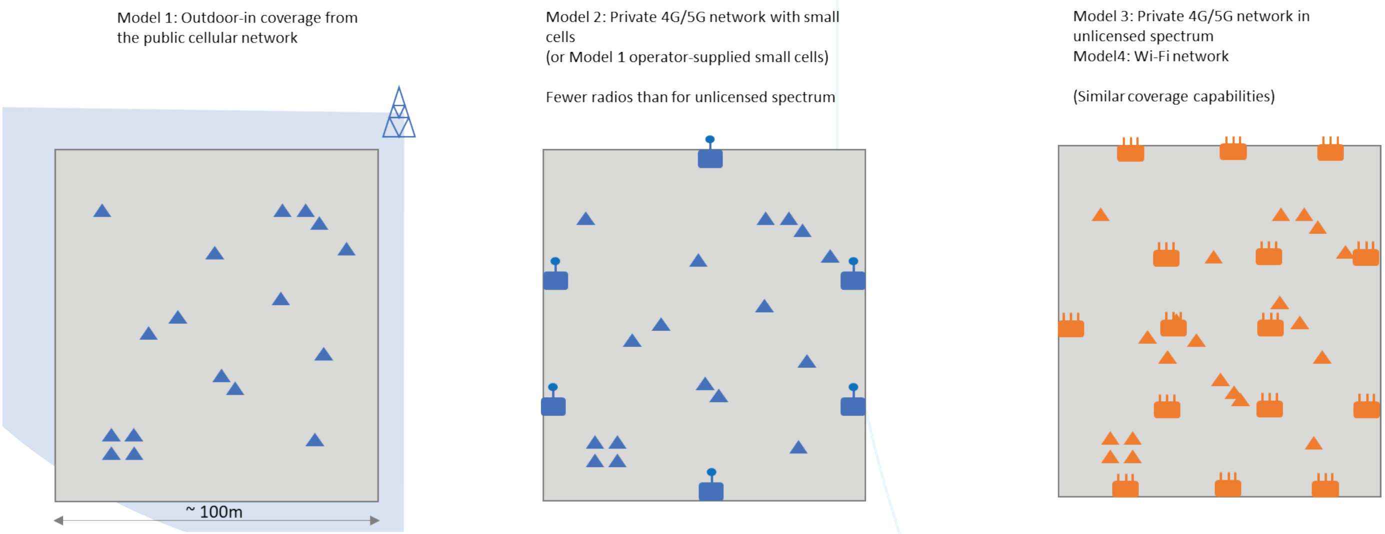
If extra 4G equipment is deemed necessary – whether for coverage, data-rate, network capacity, QoS or control reasons – small cells can be introduced to extend the 4G network inside the factory. If these small cells are owned and managed by a public cellular operator, they extend the public network. Otherwise they will form a private 4G network on spectrum acquired by the industrial end-user. For small buildings, a single small cell maybe sufficient, but in most cases a number will be installed as an indoor network, wall- or ceiling-mounted. The sensors will need modules of the same radio technology chosen for the small cells.

A private 4G network will require the end-user to install a 4G core network locally, or contract for one of the emerging cloud services as and when these become available.

Wi-Fi networks are deployed in many factory and warehouse settings, and the challenges posed by these environments are well understood. For instance, warehouses often have tall, metal or RF-absorbing racks of products, which block signals. Even cardboard packaging can be an RF-absorber in humid climates. The solution is to ceiling-mount access points over aisles, or wall-mount them at the end of aisles. One consequence of this topology is increased distance from access point to sensor device; the solution is to use one of a range of high-gain antennas to provide high-quality signals where required. 4G technology may be able to mitigate these issues by using higher-power transmitters in licensed spectrum, but RF obstacles in warehouse and factory settings will remain challenging for both Wi-Fi and 4G small cells, requiring careful RF design.

Power and backhaul can also pose obstacles in factory buildings. While backhaul can be addressed by using mesh networking between Wi-Fi access points, power from AC or power-over-Ethernet sources remains a requirement.

Wireless IoT in a factory


Model 1: Outdoor-in coverage from the public cellular network
~ 100m
Model 2: Private 4G/5G network with small cells
(or Model 1 operator-supplied small cells)
Fewer radios than for unlicensed spectrum
Model 3: Private 4G/5G network in unlicensed spectrum
Model4: Wi-Fi network
(Similar coverage capabilities)

Outdoor plant

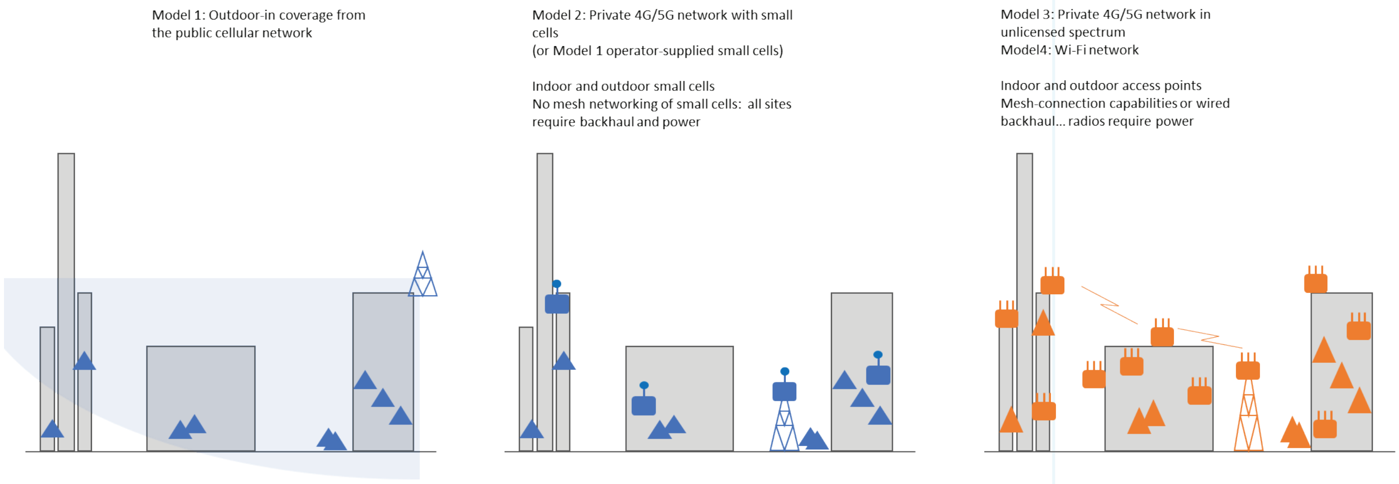
As Industrial IoT moves outdoors, to cover the large distances, isolated buildings and metal obstructions found in process and chemical plants, the need for careful RF planning increases, for both Wi-Fi and 4G technologies.

The longer range of 4G operating in licensed bands means fewer radios are required, but Wi-Fi has more flexible mesh networking options to connect isolated access points.

A 4G approach might use outdoor radio units mounted on high buildings or structures, or purpose-built towers, to serve open spaces and even some buildings with outside-in coverage. These will need to be augmented with indoor small cells for conventional buildings and areas that are shadowed by metal structures.

Wi-Fi will deploy more radio units but with focused coverage. Several access points, with high-gain directional antennas will be mounted on towers, on top of or outside buildings. It is possible to mount access points indoors, with antennas pointing through windows or mounted on the outside of the building, connected by short through-wall cables. Mesh networking allows multiple radio hops back to an Ethernet or fiber anchor-point.

Wireless IoT in an outdoor plant


Model 1: Outdoor-in coverage from
the public cellular network
Model 2: Private 4G/5G network with small
cells
(or Model 1 operator-supplied small cells)
Indoor and outdoor small cells
No mesh networking of small cells: all sites
require backhaul and power
Model 3: Private 4G/5G network in
unlicensed spectrum
Model4: Wi-Fi network
Indoor and outdoor access points
Mesh-connection capabilities or wired
backhaul... radios require power

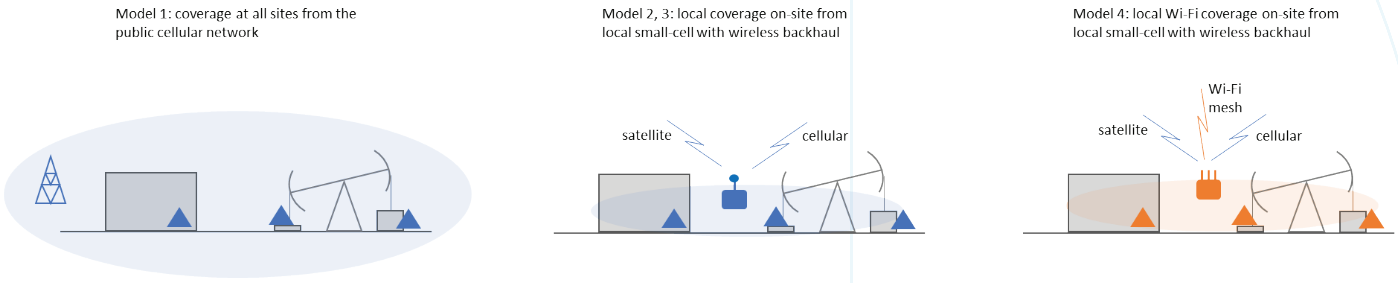
Isolated, multi-site networks

Mining and oil production organizations operating in rural areas often find they need to connect IoT networks at a large number of isolated sites. These can pose challenges, particularly if a unified network architecture is desired, as they may be outside public cellular coverage.

In such cases, the first network model above will not be adequate. Often the best solution is a 2-step network, where IoT sensors and actuators connect locally to an aggregator, using wired or Wi-Fi connections. Then the aggregator-router directs the signal over an appropriate wide-area connection, usually satellite, cellular or Wi-Fi as available. This allows the local network to be a standard design, with modular WAN options.

It should be noted that where the organization has rights of way or other points of presence, Wi-Fi can reach across long distances. Railroad owners, for example, have built very long Wi-Fi chains along their tracks, through areas that are not served by the cellular network.

Wireless IoT for isolated multi-site networking



Model 1: coverage at all sites from the public cellular network

Model 2, 3: local coverage on-site from local small-cell with wireless backhaul

Model 4: local Wi-Fi coverage on-site from local small-cell with wireless backhaul

FUTURE DEVELOPMENTS IN CELLULAR TECHNOLOGY FOR INDUSTRIAL IOT: 5G

The 5G vision is much broader than for the preceding 2G, 3G or 4G generations. For 5G, the 3GPP standards collaborators added many more dimensions to the specifications, enabling equipment designers and network architects to build a wide variety of networks covering almost every type of public and private architecture seen today. As we will discuss later, it is still an open question whether today's mobile operators will be willing to make the organizational and process changes necessary to take advantage of these opportunities, or even if the business cases will be competitive against current private networking technologies such as Wi-Fi. Hence, the majority of 5G standards will never be used in real networks, but it is impossible to predict today which will prove useful and which will be discarded. In this paper we are concerned with factory and process plant IoT networking - first, we consider the 4G/5G building blocks for Industrial IoT.

5G New Radio

The first new 5G improvement is in radio technology. As the marketing departments of mobile operators compete with each other, the definition of '5G' will be stretched to include many 4G-LTE standards, so we will deal with all 'new' radios under this heading. 5G allows the radio to extend to both lower and higher data-rates, and adds the possibility of limiting latency and enhancing reliability, both aspects of QoS that are important for Industrial IoT.

1) At the low-rate end, we have already identified NB-IoT and LTE Cat-M1 as IoT radio technologies. Both can be implemented as extensions of the 4G network, allowing significant scaling-up of device numbers while potentially reducing the cost-per-bit so service providers can reduce subscription charges to the level where sensor fleets become cost-effective. When the public cellular network can support millions of inexpensive sub-150 kbps connections in this way, it becomes attractive for IoT applications: connected-cars, meter-reading, and the like. Cars and commercial vehicles are especially good candidates for these technologies because they require the extensive wide-area coverage of the cellular network for nearly-always-available connections.

2) At the other end of the scale, 5G takes existing 4G techniques such as channel aggregation and MIMO, and extends them to increase the theoretical top data-rates of 5G into the Gbps. Average rates in the public network will be far below this, but if mobile operators start to build-out custom transmitter sites for specific enterprises, the potential for a very-high-capacity network of dense, high-rate connections is available, and this may be attractive for industrial users.

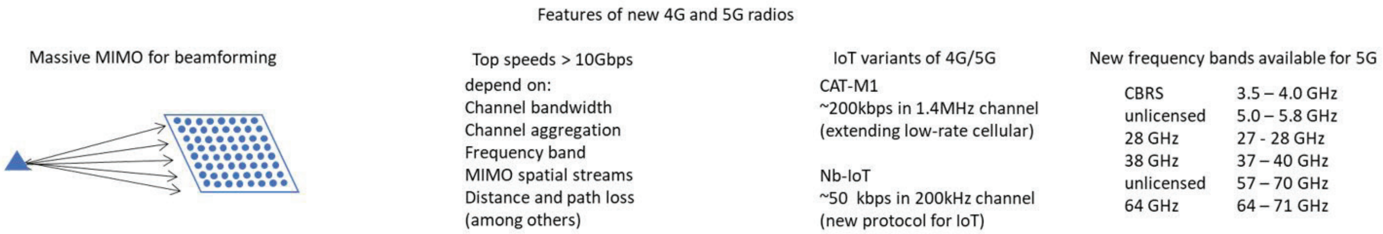
3) The other new radio aspects of 5G revolve around latency and reliability. These will be quite difficult to achieve in practical networks; they are best thought of as standards-based building-blocks for increasing network performance. Latency, for example, is an end-to-end network parameter, and while the 5G radio allows over-the-air latency to be reduced to theoretical levels in the 10 - 50 msec range, skilled network designers will be required to avoid other sources of latency creeping in elsewhere. In the type of network discussed here, the mobile operator will provide these skills.

4) Another new dimension of 5G is spectrum allocation and use. There is a world-wide coordinated effort by regulators to open up new spectrum for 5G networks. While some is in low- and mid-bands, up to 6 GHz with similar characteristics to today's cellular and Wi-Fi networks, most of the new spectrum is around 28, 39 and 60 GHz frequencies. These, and neighboring bands, have been used for point-to-point networks for many years, and their characteristics for this are well-known. Indeed, the first commercially deployed 5G radios will be point-to-point, mobile-broadband-to-the-home-over-wireless networks using these frequencies. But high-frequency radio for mobile devices is much more difficult to control than lower bands, as the Wi-Fi ecosystem has found with WiGig in the 60 GHz band, and while there is much speculation, it remains to be seen how much of this spectrum will be useful – and actually used - for mobile networking. The proliferation of frequency bands also brings complexity to device makers. Even with 4G, most consumer devices are designed with a subset of the various LTE bands, as it is too complicated and expensive to incorporate universal multi-band support – different antennas and radio frequency front-end components – in a small form-factor at a reasonable price point. With 5G these constraints will become more severe, particularly for low-cost IoT sensors, and it is likely that particular devices will be limited to a subset of geographies, bands and network operators.

5) The range of cellular links compares well with Wi-Fi: in 4G networks, fewer base stations are needed to cover a given area, so cells are larger. This is due to two factors. The spectrum used in 4G is lower frequency than Wi-Fi, so signals propagate more easily. Further, the licensing rules for the spectrum allow for higher transmit power at the base station. These are the reasons fewer 4G small cells are needed to cover a building than Wi-Fi access points. These advantages will probably continue to hold in the 5G era, although the use of high-frequency spectrum would negate the propagation advantage. But the cost of high-power transmitters, if used, will be a significant economic factor.

6) The 5G standards also allow multiple QoS priorities to be specified and tailored to respective application needs. These are indeed significant capabilities, but the most difficult parts of QoS are for customers to identify and specify their traffic needs, and network engineers to build the mechanisms to drive these requirements into network configurations: Today's cellular network offers just one QoS level, so significant changes will be required to support differentiated access.

7) These and various other aspects associated with the radio interface – data-rates, spectral efficiency, performance, QoS and security among others – have been proposed as differentiators between 4G and 5G, and between cellular technologies and Wi-Fi. Some comparisons of cellular technology in these areas claim technical superiority over Wi-Fi, but in fact the underlying radio technologies are now very similar, with few significant differences – the two aspects where 5G has an edge are in wide-area coverage, due to the cellular network, and high-speed mobility, at greater than 70 km/hr: the other differences are marginal. We discuss the respective waveforms and show detailed comparisons in a companion technical paper.



Features of new 4G and 5G radios

Massive MIMO for beamforming

Top speeds > 10Gbps
depend on:
Channel bandwidth
Channel aggregation
Frequency band
MIMO spatial streams
Distance and path loss
(among others)

IoT variants of 4G/5G
CAT-M1
~200kbps in 1.4MHz channel
(extending low-rate cellular)

Nb-IoT
~50 kbps in 200kHz channel
(new protocol for IoT)

New frequency bands available for 5G

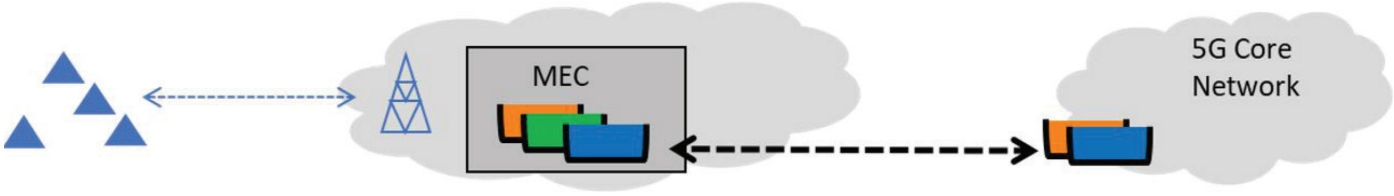
CBRS	3.5 – 4.0 GHz
unlicensed	5.0 – 5.8 GHz
28 GHz	27 - 28 GHz
38 GHz	37 – 40 GHz
unlicensed	57 – 70 GHz
64 GHz	64 – 71 GHz

Other 5G components

The remaining innovations introduced by 5G are in data processing and control behind the radio, in the operator's core network. One of the fastest to market is likely to be 'edge computing' as it is generally known, or MEC (Multi-Access Edge Computing) in 3GPP terms. MEC is a new concept which can be thought of as countering the drawbacks of the previous innovation wave, cloud computing. While the cloud has well-established benefits, it has become apparent that it brings two major problems.

3) ETSI, a standards body founder of the 3GPP, is working on standards for the MEC to be applied in 5G networks. The MEC is a computing platform located at the edge of the 5G network, close to where data is generated and consumed. It provides a platform where data-center applications can be downloaded to meet the data and process it, all under a control framework that can be coordinated and managed

Multi-Access Edge Computing (MEC)



1) The first problem is latency. While the cloud decouples computing functionality from its physical location, there are some applications where round-trip-time is important and must be limited. An oft-quoted example is where images or video must be processed in real-time, for instance on a manufacturing line or for personnel access-control. For cases where an answer must be provided in hundreds of milliseconds, it is acceptable to ship the data across a continent for processing in a distant data center, as can be the case for cloud networks.

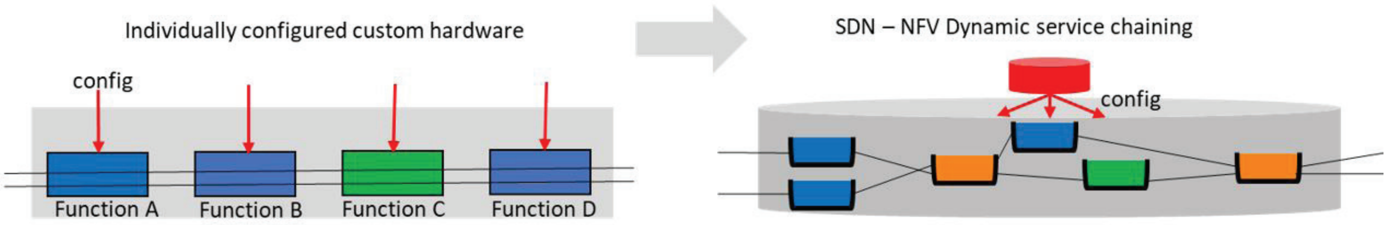
2) Secondly, some applications, notably video, produce such quantities of data that sending an uncompressed stream across the Internet to a cloud provider may run into network bottlenecks, and will certainly clock up expensive bills with the cloud provider. In both cases, the answer is to process the data locally, as close as possible to where it is produced, providing faster access to the source and compressing the data before sending it over the Internet.

It is clear that one of the more significant challenges with MEC is in control – 'orchestration' in 3GPP terms – of the various devices and computing workloads. Something needs to recognize that a sensor requires service execution nearby, configure the sensor to point to an appropriate MEC instance, and download the correct application software to the MEC to meet the sensor's needs. This is a complex problem. But it can be solved, and as general-purpose edge-computing is already making progress in the private networking market, its extension to operator-specific 5G architecture is a small jump.

The next innovation in 5G can be called 'software everywhere'.

For the last few years, the large mobile operators have been developing a concept where services were not built from different vendors' 'boxes' where each box is a customized hardware-software platform, but by chaining together software functions from different vendors, an architecture known as NFV (Network Functions Virtualization).

Software Defined Networking + Network Functions Virtualization


Individually configured custom hardware
config
Function A
Function B
Function C
Function D
SDN – NFV Dynamic service chaining
config

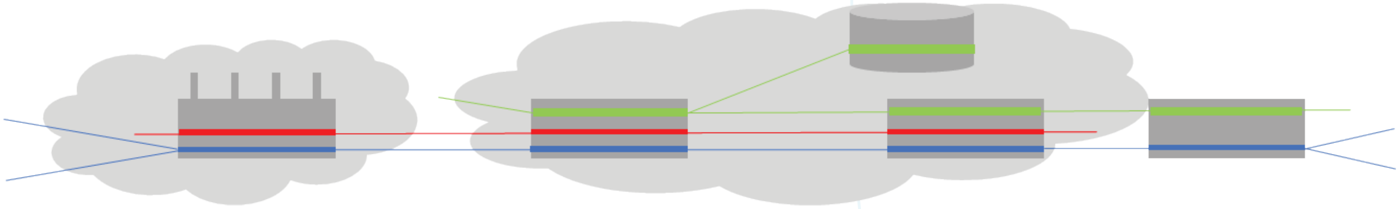
1) While the evolution of NFV has been much slower than originally expected, it is generally accepted that the future mobile operator network core will eventually run on general-purpose virtualized computing platforms where applications are spun-up and interconnected to form services dynamically. This means the network can be re-configured in an infinite number of ways through software control. But that control function is complex and has become a new market in its own right.

2) Another aspect of software everywhere is a new form of network management with more powerful APIs (Application Programmable Interface) to manage the operator's infrastructure, a function broadly known as SDN (Software-Defined Networking).

3) These software control and management functions are critical to mobile operators' moves into the enterprise market because they allow fine control of network functionality. Today's cellular networks support only one class of service for consumer devices, and operators find it hard with current management tools to maintain even this basic level of sophistication. If they are to service enterprises, they will need to identify and configure many classes of service on diverse devices, and monitor and troubleshoot this population on a single network. This will require ever-higher levels of network abstraction and visualization, a task for the next generation of software.

Network Slicing. Once the mobile operator has a 5G management and orchestration layer, and an SDN/NFV network with software- rather than hardware-based execution, it can implement the next level of QoS for enterprise networks.

Network Slicing



1) The Network Slicing concept is new for 5G. It involves reserving capacity across the network for specific services or customers. For example, if an enterprise wished to build a high-performance video conferencing service across the public cellular network, it could specify requirements such as bandwidth, latency and limited connection topology and deliver these specifications as a bundle to the mobile operator. The operator would then configure its network so those resources were always available to that customer for that application, end-to-end.

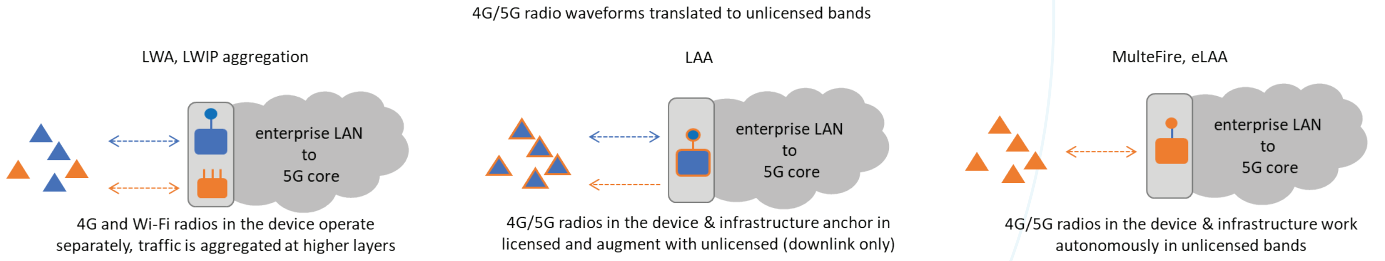
2) This concept requires a very high degree of visibility and control in the mobile operator's network, and a multi-tenant function where specific customers and services can be identified and linked to their respective execution blocks in the infrastructure. While easy to draw on slideware, it is a very complex requirement in terms of configuration, service ordering and billing. While new 5G equipment will become Network-Slicing-ready over time, it remains to be seen how successfully network operators implement the required functionality.

3) For an Industrial IoT customer, the benefits of Network Slicing are obvious. It provides a virtual-private-network function that is used to guarantee service levels over a shared network, and can be used for security purposes to prevent mixing of public and private traffic over the network. It is a pre-requisite for the type of Industrial IoT network envisaged by the 5G project.

5G will extend the use of unlicensed spectrum. Developments over the last 5 years have marked an extraordinary departure for the cellular industry and 3GPP. After insisting for many years that operator-exclusive licensed spectrum was required in order to deliver a high-quality service, equipment vendors and operators proposed an initiative that allowed cellular networks to extend into the unlicensed bands used by Wi-Fi and others. This move was prompted by a general shortage of licensed spectrum in some areas, as well as the (much lower!) cost of unlicensed spectrum.

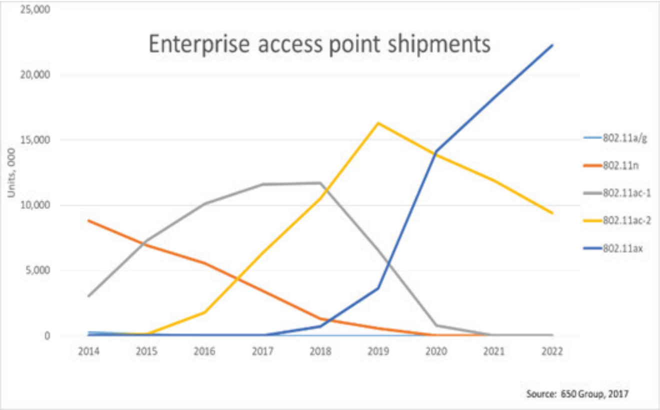
The first 3GPP use of unlicensed spectrum, LAA (License-Assisted Access) is a multi-channel protocol. It requires an 'anchor' connection in licensed spectrum where control traffic flows, but uses channel-bonding to extend the downlink into the 5 GHz band when requested by the base station.

While LAA is already gaining widespread use in the public cellular network, it is generally used outdoors in city centers and the macro network, where the amount of cellular traffic can overwhelm the limited licensed spectrum available: its applicability to indoor networking is questionable. It is of general interest because the use of unlicensed spectrum for cellular traffic has the potential to reduce the amount of bandwidth available for co-located Wi-Fi networks, and because it is not yet clear how 'polite' LAA may be as a neighbor: will it share frequencies fairly, or tend to hog bandwidth and constrict overlapping Wi-Fi WLANs? There is not yet enough LAA traffic in real networks to measure these effects.


4G/5G radio waveforms translated to unlicensed bands
LWA, LWIP aggregation
enterprise LAN
to
5G core
4G and Wi-Fi radios in the device operate separately, traffic is aggregated at higher layers
LAA
enterprise LAN
to
5G core
4G/5G radios in the device & infrastructure anchor in licensed and augment with unlicensed (downlink only)
MulteFire, eLAA
enterprise LAN
to
5G core
4G/5G radios in the device & infrastructure work autonomously in unlicensed bands

NEW DEVELOPMENTS IN WI-FI FOR INDUSTRIAL IOT: WI-FI 6

Wi-Fi is by now the established way to access the Internet, whether at home or at work, from PCs or cellphones. In 2019, 20 years after the first meeting of the Wi-Fi Alliance, Wi-Fi will carry more than 50% of all Internet traffic. With around 8 billion Wi-Fi devices in use, and 3 billion new ones being added every year, it is difficult to find anywhere without a Wi-Fi signal, and even cellphone networks, which have been improving speeds and capacities with the LTE build-out, small cells and flat-rate data plans rely on Wi-Fi to meet the traffic requirements of their subscribers. A cellphone today without integrated Wi-Fi would be unthinkable.

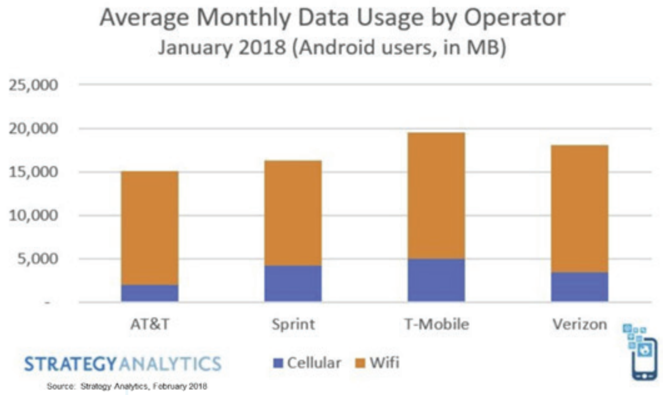


Source: 650 Group, 2017

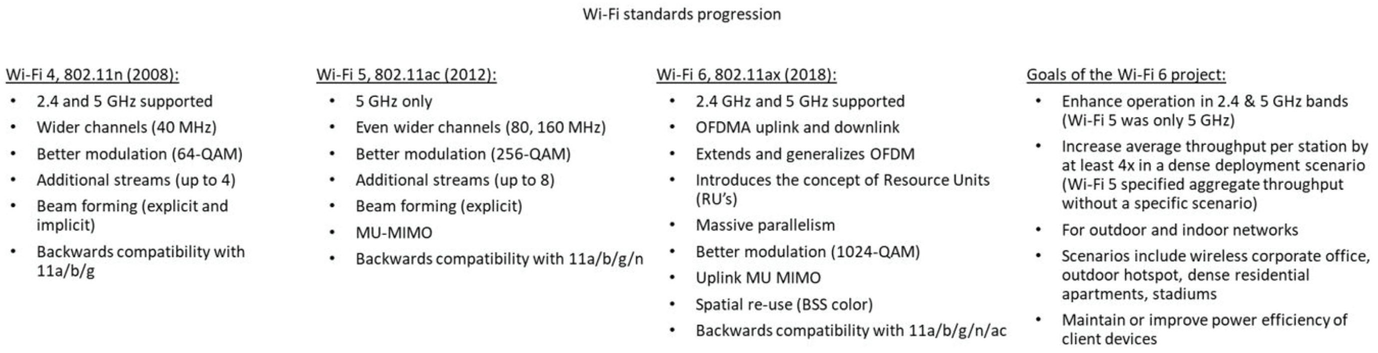
Wi-Fi is also well-established in industrial settings, helping to automate manufacturing industry, agriculture, food and beverage plants and in many other settings.

The next advance, Wi-Fi 6, is already shipping. It will raise the performance bar yet again for the sixth generation of Wi-Fi (the Wi-Fi Alliance now calls 802.11ax "Wi-Fi 6"). The traditional techniques used in Wi-Fi 4 and Wi-Fi 5 – wider RF channels, more MIMO antennas, higher QAM modulation – have been pushed almost to the limit, so the new standard incorporates other ideas that make it better-suited to emerging market opportunities.

Several less-publicized features improve range, power consumption and scale to make Wi-Fi a better match for IoT requirements



Source: Strategy Analytics, February 2018



Wi-Fi standards progression

Wi-Fi 4, 802.11n (2008):

- 2.4 and 5 GHz supported
- Wider channels (40 MHz)
- Better modulation (64-QAM)
- Additional streams (up to 4)
- Beam forming (explicit and implicit)
- Backwards compatibility with 11a/b/g

Wi-Fi 5, 802.11ac (2012):

- 5 GHz only
- Even wider channels (80, 160 MHz)
- Better modulation (256-QAM)
- Additional streams (up to 8)
- Beam forming (explicit)
- MU-MIMO
- Backwards compatibility with 11a/b/g/n

Wi-Fi 6, 802.11ax (2018):

- 2.4 GHz and 5 GHz supported
- OFDMA uplink and downlink
- Extends and generalizes OFDM
- Introduces the concept of Resource Units (RU's)
- Massive parallelism
- Better modulation (1024-QAM)
- Uplink MU MIMO
- Spatial re-use (BSS color)
- Backwards compatibility with 11a/b/g/n/ac

Goals of the Wi-Fi 6 project:

- Enhance operation in 2.4 & 5 GHz bands (Wi-Fi 5 was only 5 GHz)
- Increase average throughput per station by at least 4x in a dense deployment scenario (Wi-Fi 5 specified aggregate throughput without a specific scenario)
- For outdoor and indoor networks
- Scenarios include wireless corporate office, outdoor hotspot, dense residential apartments, stadiums
- Maintain or improve power efficiency of client devices

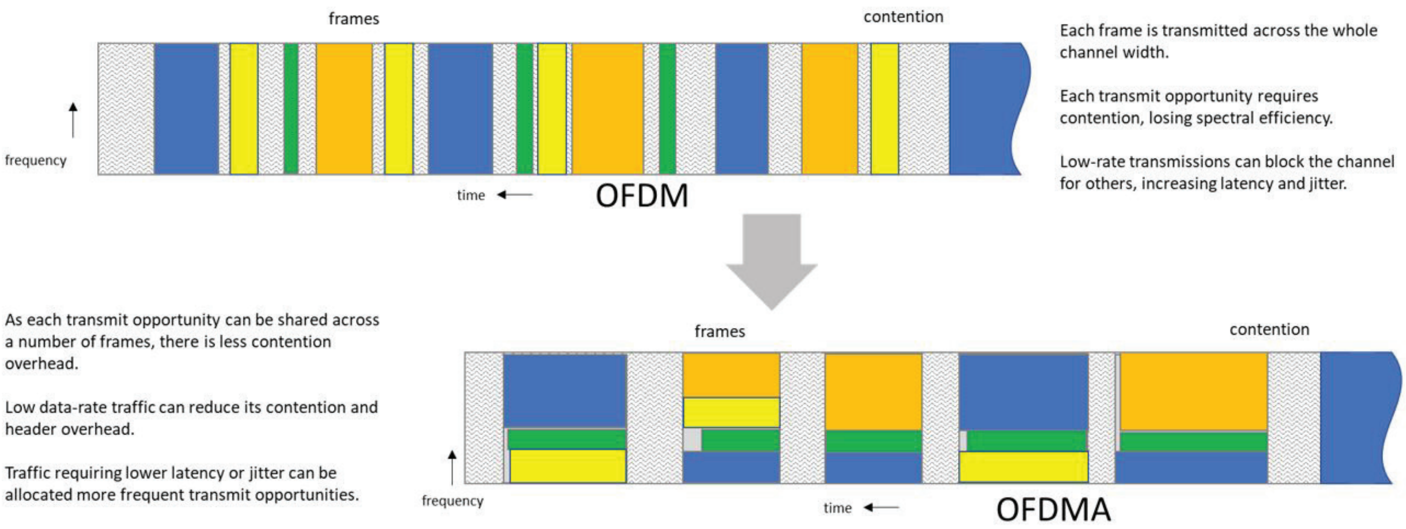
The Internet-of-Things is an important new market, and extends the performance envelope established for past automation projects. As established earlier in this document, the important metrics for an IoT device in this environment are data rate, range, power consumption, security, ease of configuration, and scale. Wi-Fi 6 has new features that improve all of these performance dimensions, making Wi-Fi a more attractive choice for connecting IoT devices in enterprise environments.

Whereas the mainstream Wi-Fi application – streaming high-speed Internet signals to PCs, tablets and smartphones – requires high data rates over relatively short distances, IoT can usually use low speed connections, often in the sub-Megabit range.

The new OFDMA (Orthogonal Frequency Division Multiple Access) feature allows sub-channelization to reduce the lower data rates to sub-2 Mbps, while extending the number of individual devices that can be reliably supported on an access point, into the thousands. This addresses the data rate and scale requirements of enterprise IoT.

OFDMA is one of two multi-user modes in Wi-Fi 6, the other being MU-MIMO. OFDMA is a technique that has been used in other systems, like cellular-LTE, for many years. It works by dividing a transmission across the frequency dimension, with pairs of devices assigned to transmit and receive in sub-channels or Resource Units (RU's) of the main RF channel.

OFDMA compared with single-user OFDM



Each frame is transmitted across the whole channel width.

Each transmit opportunity requires contention, losing spectral efficiency.

Low-rate transmissions can block the channel for others, increasing latency and jitter.

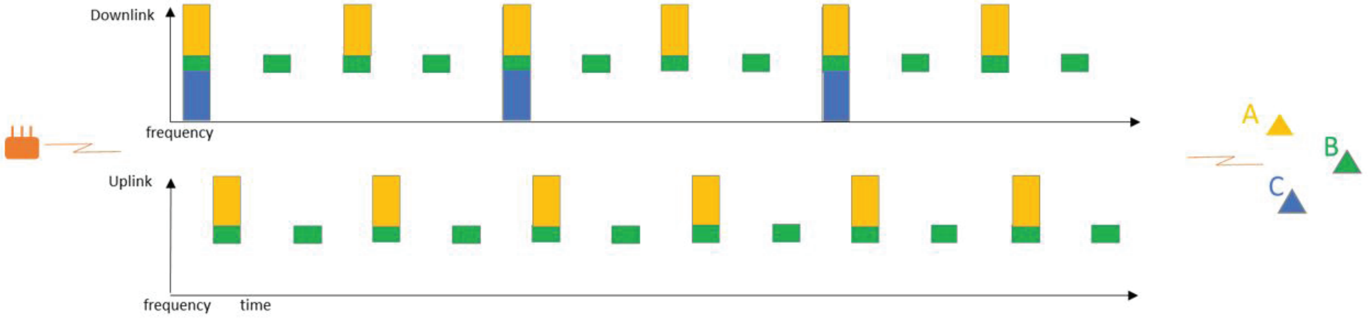
As each transmit opportunity can be shared across a number of frames, there is less contention overhead.

Low data-rate traffic can reduce its contention and header overhead.

Traffic requiring lower latency or jitter can be allocated more frequent transmit opportunities.

This allows an access point (for downlink OFDMA) to bundle several frames together in different sub-channels in a single transmit opportunity, while its clients tune their radios to different sub-channels to receive their respective transmissions. OFDMA is especially useful in managing large numbers of clients fairly, and a reduction in contention overhead means there is little deterioration in capacity as client numbers increase.

OFDMA example: deterministic rate and delay, minimal jitter (simplified view)

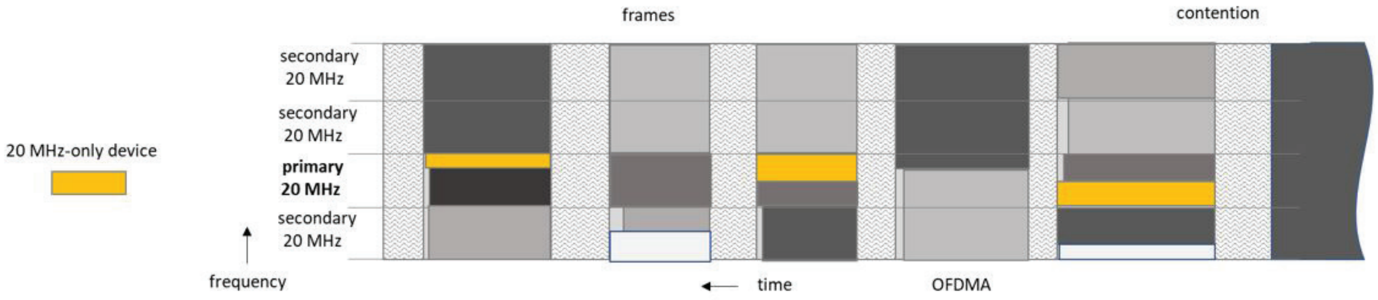


- Transmit opportunities are controlled and scheduled by the AP for both uplink and downlink, independently (C is shown as downlink only).
- Example: Transmit opportunities every 5msec, for 1.5msec in a 20MHz channel
  - A, C: 106 subcarriers, rate = 8 Mbps x 1.5/5/2 = 1.2 MHz bandwidth full duplex with max 10 msec latency, < 1 msec jitter. @MCS9, 256-QAM 3/4 = ~6.6 Mbps each way
  - B: 26 subcarriers, rate = 2 Mbps x 1.5/5 = 600 kHz bandwidth full duplex with max 5 msec latency, < 1 msec jitter. @MCS6 64-QAM 5/8 = ~2.2 Mbps each way
- For given range & noise conditions, lower data rate -> lower error rate, for full control.
- Allows space between scheduled frames for opportunistic contention for bursty traffic.

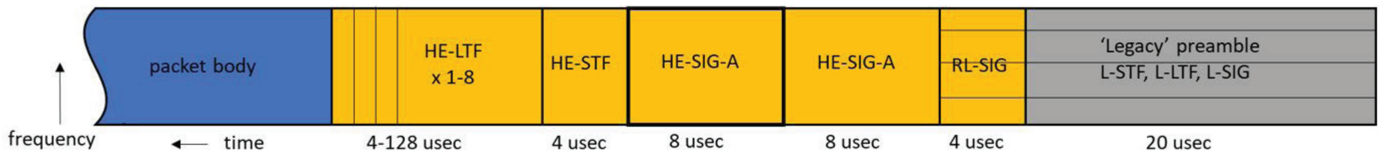
There are also advantages for less-capable stations. As link-speeds have increased, some devices struggle to transmit at the maximum rates. Whereas with full-channel OFDM, they have to do the best they can, perhaps not filling the medium, OFDMA allows them to cap their maximum rates. This allows for simpler hardware implementations and potentially longer battery life.

Another feature introduced for IoT sensors is the '20 MHz-only' class of device. This seeks to reduce complexity, leading to lower-power, lower-cost chips. A 20 MHz-only device is capable of operating in either the 2.4 or the 5 GHz band, but only in 20 MHz at a time, on the designated primary channel. It supports nearly all other mandatory features, including OFDMA options, allowing such a device to transmit and receive on a much smaller sub-channel.

20 MHz-only operation



Single-user extended-range frame



Always transmitted in 1 spatial stream, at MCS0, MCS1 or MCS2 modulation

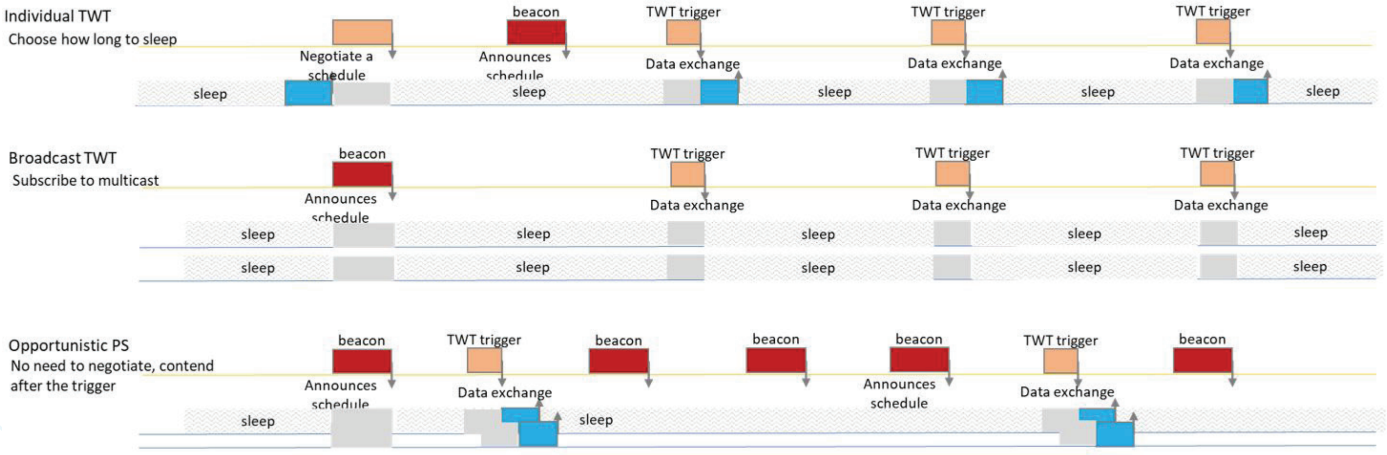
But the connection must also work over longer distances, to ensure coverage throughout the building and beyond with good reliability. Wi-Fi 6 includes several features that extend range, both explicitly through extra redundancy in key parts of headers, and implicitly in features such as OFDMA, where range can be improved at the lower data rates.

Meanwhile, it is often impossible or inconvenient to run cabling to sensor locations, so many IoT devices are battery-powered, making power consumption a key consideration. Here, Wi-Fi 6 has several features to drive down power requirements. TWT (target wait time) allows a client device to sleep for long periods, setting a future time to wake and contact the access point. This is useful when an IoT device has few frames to send and receive at long intervals, meeting the requirement for infrequent but reliable communication. Also, several new options in the specification are intended to drive a new product line of small-footprint, limited-function chips targeted for the IoT market, designed to achieve the lowest power consumption needed to meet the IoT performance envelope.

Since most IoT devices are headless with no keypad or display, fast, bulk configuration for connectivity and security are important requirements. While not part of the Wi-Fi 6 standard, the Wi-Fi Alliance has a new certification, "Easy Connect" that incorporates QR-code scans and other simple identifiers in a cryptographically-secure protocol.

Connectivity is a small but important part of the overall Industrial IoT system, and these changes in Wi-Fi 6 are intended both to enable new IoT applications, broadening the use-cases for IoT, and also to make Wi-Fi a more attractive choice when compared to the other low-rate, low-power IoT wireless protocols used in enterprise applications: BLE (Bluetooth Low-Energy) and IEEE 802.15.4 extensions such as ZigBee. In today's equipment, Wi-Fi already offers the highest data rates and excellent security, but with limited range and complex configuration, while the other technologies are not, in practice, as secure, but are less expensive to incorporate into sensor hardware, and – most important – have low enough power consumption to run on button cells for many months or years. Wi-Fi 6 allows Wi-Fi to narrow these gaps in the system envelope, extending its applicability in the IoT ecosystem.

TWT power-save options in Wi-Fi 6



RELIABLE INDUSTRIAL WIRELESS NETWORKS

Reliability is a critical concern for many wireless networks, and an organization setting out to build a control or monitoring network should consult experts for advice. The following notes identify some of the key aspects of private 4G and Wi-Fi networks.

For the very highest reliability, it is usually best to go with a wired or fiber connection if possible – all wireless networks are vulnerable to interference, whether intentional or unintentional. But mobility and other operational parameters may direct organizations to a wireless network for high-reliability applications.

The network should be designed with appropriate levels of redundancy. Most high-reliability networks will use some form of uninterruptable power supply to guard against power failures. For both Wi-Fi access points and 4G small cells, the usual architecture will be to power the radio units with Power-over-Ethernet, and provide redundant power and Ethernet in the switches driving the radios.

All enterprise WLAN and 4G small cell vendors have architectures that provide redundancy for equipment failure. This will include overlapping radio coverage, so the failure of any radio unit is not catastrophic, and 1:1 or 1:N redundancy of functions such as WLAN controllers or Radio Access Network control units. Redundant radios in client units are another consideration when designing high-reliability networks.

If wide-area connections are part of the critical path, it is usual to provision alternate paths, for instance satellite or public cellular connections can take over from wired WAN connections in the event of an outage, even if they support lower-rate connections.

All the points above are equally applicable to private 4G and Wi-Fi networks.

Interference is an important consideration for wireless networks. 4G networks in licensed spectrum have strong guarantees against interference from overlapping, intentional transmitters using the same RF channel. Networks in unlicensed spectrum, such as Wi-Fi, have no such guarantees, but given the short-range nature of Wi-Fi, organizations whose networks are some distance from public areas have some assurance that strong interfering signals are very unlikely – they effectively control their own air-space.

And even licensed spectrum is subject to unintentional, or malicious interference or jamming. This possibility must be part of any network reliability assessment, particularly where industrial machinery is operating. One way to mitigate this risk is for the network to be frequency-agile, able to detect interference and dynamically and/or autonomously switch to a clear channel. Enterprise WLANs have such features as part of their interference-detection and channel-selection capabilities.

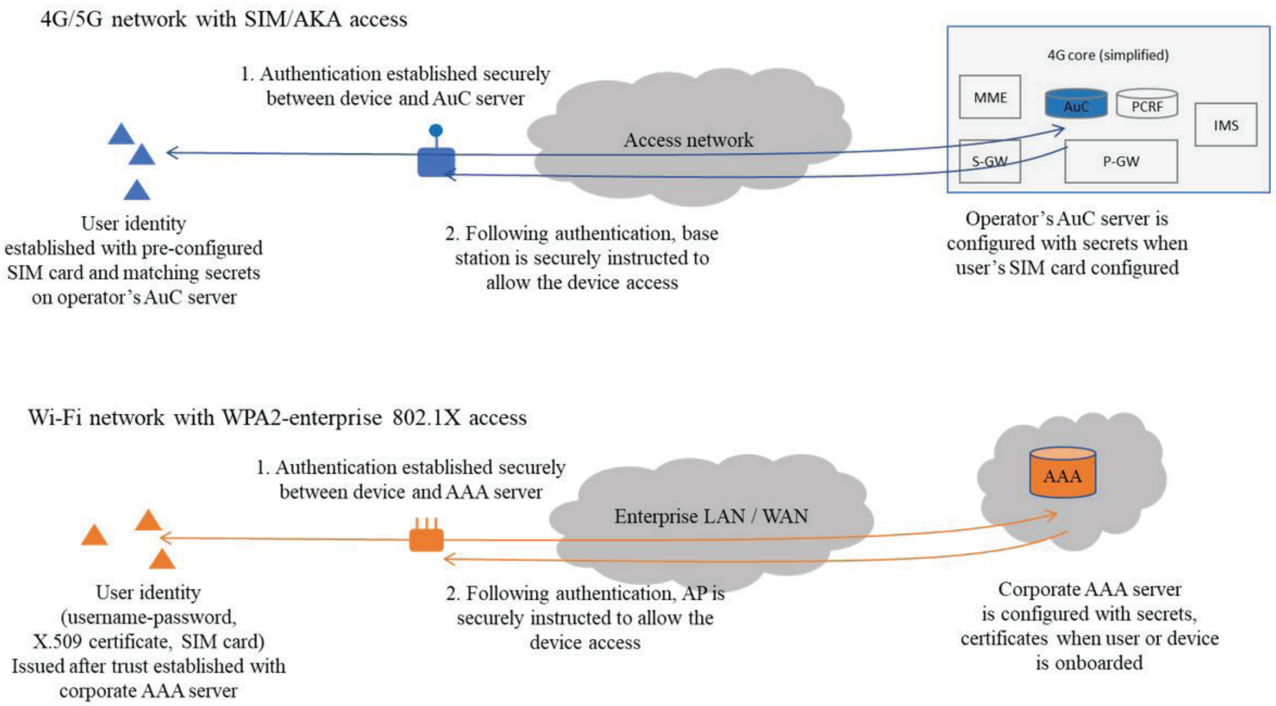
CBRS is an interesting hybrid of licensed and unlicensed spectrum. On the one hand, an organization gaining a PAL (Priority Access License) for a 10 MHz channel is assured that no other PAL or lower-tier users can use that channel. On the other hand, the organization should satisfy itself that incumbent-tier band users, i.e., US military users will not appear in the channel and pre-empt all transmissions, as this would impact the network's availability. The likelihood of pre-emption will depend on geography and other factors.

Even moving to the public cellular network may not improve reliability over a well-designed private network. All public cellular networks have experienced outages over the years, often due to software upgrades introducing problems, or the unexpected failure of a critical function within the network. Well-designed wireless networks are very reliable, but they cannot be infallible.

SECURITY

A user or device presents its identity to the network as a first step for authentication. The form and flexibility of identities supported by the network is important. IoT devices are usually small and headless, so it is important that they use an authentication form that is physically small and preferably embedded in the device. Organizations managing private fleets of IoT devices need to acquire tools and build processes to program each device with a unique identity, keep track of the binding between identity and device name, function and location, and set up an appropriate AAA (Authentication, Authorization and Accounting) server in their data center to handle authentication functions.

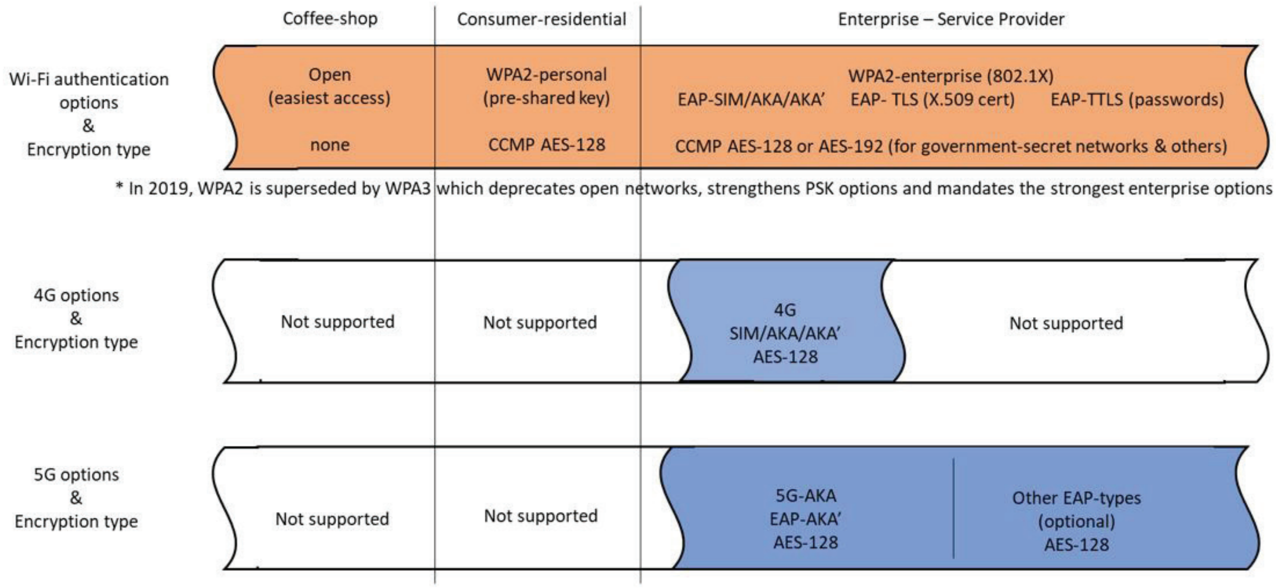
4G/5G authentication architecture compared to Wi-Fi


4G/5G network with SIM/AKA access
1. Authentication established securely between device and AuC server
Access network
4G core (simplified)
MME
AuC
PCRF
IMS
S-GW
P-GW
User identity established with pre-configured SIM card and matching secrets on operator's AuC server
2. Following authentication, base station is securely instructed to allow the device access
Operator's AuC server is configured with secrets when user's SIM card configured
Wi-Fi network with WPA2-enterprise 802.1X access
1. Authentication established securely between device and AAA server
Enterprise LAN / WAN
AAA
User identity (username-password, X.509 certificate, SIM card) Issued after trust established with corporate AAA server
2. Following authentication, AP is securely instructed to allow the device access
Corporate AAA server is configured with secrets, certificates when user or device is onboarded

The 4G network uses a SIM card as the device identifier. A SIM is tamper-resistant and now available in embedded-chip eSIM form: the SIM and the authentication method used are proprietary to the 3GPP. The authentication framework has been upgraded over the years, and now SIM authentication (although not the SIM card itself) is deprecated, as it is known to be vulnerable to attacks, in favor of the AKA ('Authentication and Key Agreement') and AKA' protocols.

As networks evolve from 4G to 5G, the 3GPP is retaining AKA authentication and SIM identity, but allowing options (as 'secondary authentication for data networks outside the mobile operator domain') for EAP-framework security, the same structure that has been available in Wi-Fi for 15 years.

4G/5G security compared to Wi-Fi



	Coffee-shop	Consumer-residential	Enterprise – Service Provider
Wi-Fi authentication options & Encryption type	Open (easiest access) none	WPA2-personal (pre-shared key) CCMP AES-128	WPA2-enterprise (802.1X) EAP-SIM/AKA/AKA' EAP- TLS (X.509 cert) EAP-TTLS (passwords) CCMP AES-128 or AES-192 (for government-secret networks & others)
4G options & Encryption type	Not supported	Not supported	4G SIM/AKA/AKA' AES-128 Not supported
5G options & Encryption type	Not supported	Not supported	5G-AKA EAP-AKA' AES-128 Other EAP-types (optional) AES-128

* In 2019, WPA2 is superseded by WPA3 which deprecates open networks, strengthens PSK options and mandates the strongest enterprise options

Wi-Fi, because it is used in different settings, has evolved with a broad range of security options. Some are used in retail settings and coffee-shops, others by consumers in their homes. At the high-security end of the spectrum, the security protocol for enterprise WLANs is WPA2-enterprise. This uses the IETF standard EAP-framework with individual device credentials and centralized AAA RADIUS servers. EAP allows devices to authenticated with passwords, X.509 certificates, or SIM cards.

Encryption, while part of the security framework, is separate from authentication. Again, Wi-Fi has a range of options, and the encryption used in enterprise WLANs is 128- or 192-bit AES, which meets and exceeds the encryption strength of 4G and 5G networks. The more sophisticated security options in the standard WPA2 protocol have been certified by governments for military and secret use for many years. All Wi-Fi customers can configure the same levels of security on their enterprise WLANs.

CONCLUSION

The Industrial IoT market is in its infancy, but there is much excitement, as it is now clear that the vision can indeed be realized in practical networks, and soon. But, while the feasibility of large-scale Industrial IoT is now unquestioned, the best way of building systems is not yet clear. As for the broader IoT market, many technologies and protocols can play a part the overall architecture, and it will take several years to determine the best recipe for different network types.

Several disciplines are required to build an Industrial IoT system. The sensors themselves must be miniaturized and often battery-powered; the network must provide universal, seamless and secure connectivity; edge computing will be required in many cases, to process data close to the sensor for fast response; and big-data techniques will need to be combined with machine learning – artificial intelligence to gain the best analytical insights. Each layer of this model is a market in itself, with competing companies and technologies. While Hewlett Packard Enterprise is active across the entire system and can deliver comprehensive end-to-end solutions, our focus in this paper has been on the wireless connectivity required to connect sensors over the ‘last hop’ to the nearest node of the wired backbone network.

Wi-Fi is a well-established networking technology for all kinds of private networks, ranging from consumer residential to top-secret government settings and including Industrial IoT. It is widely-known, but due to its many options its capabilities are sometimes misunderstood. For example, when configured for enterprise use, it has very strong authentication and security, and is capable of strong QoS.

Wi-Fi benefits from a wide-range of compatible IoT, consumer and specialized enterprise devices, and expertise for network installation and operation is widely-available. Because it operates in unlicensed spectrum, it can be installed in any industrial setting. Many other aspects of Wi-Fi networking were explored in this paper.

Some types of Industrial IoT network may present challenges for Wi-Fi. These areas are: where client devices are moving at speed; and when operating over long distances without opportunities for intermediate repeaters. Even these cases can be supported with alternate backhaul technologies.

Meanwhile, alternative wireless technologies for Industrial IoT are suggested by vendors of cellular equipment. These are a mix of 4G and 5G technologies following standards from the 3GPP. They show considerable promise but are immature. Although many of the techniques are from the 4G generation and have been available for some years, they have yet to make significant inroads in the Industrial IoT market, and very few commercial networks are installed.

But the 5G standards provide many more tools for this approach, where technology and equipment are borrowed from the public cellular network and re-purposed to build networks in licensed spectrum. There are several architectures for applying these techniques to Industrial IoT; each has advantages and disadvantages. In this paper we divided them into three models.

The first model is to attach IoT sensors to the existing cellular network as clients. This has advantages of near-universal coverage and well-understood behavior. But network planners should verify that their chosen operator has sufficient network coverage and capacity for the chosen radio technology at all sites they wish to enable. They may wish to verify inter-operator roaming or international availability, and if they have special needs such as QoS or enhanced coverage, they should investigate the operator’s responsiveness to single-customer requirements.

The increased flexibility of custom-built networks opens the second network model, where a private cellular network is built to cover company locations. As we discussed in the paper, the most significant obstacle here is likely to be the availability and cost of licensed spectrum.

The next significant enabling event for spectrum may be the auction and opening of the CBRS band in the US, but this will not happen before the end of 2019 and there are many unknowns to this initiative. After spectrum, sensor devices must be identified, and infrastructure equipment sourced. Since this is likely to be down-sized cellular network equipment, it may not be optimized for private network use along cost or complexity dimensions. Although it has been possible to build this type of network with 4G technology for some years, few commercial networks are installed.

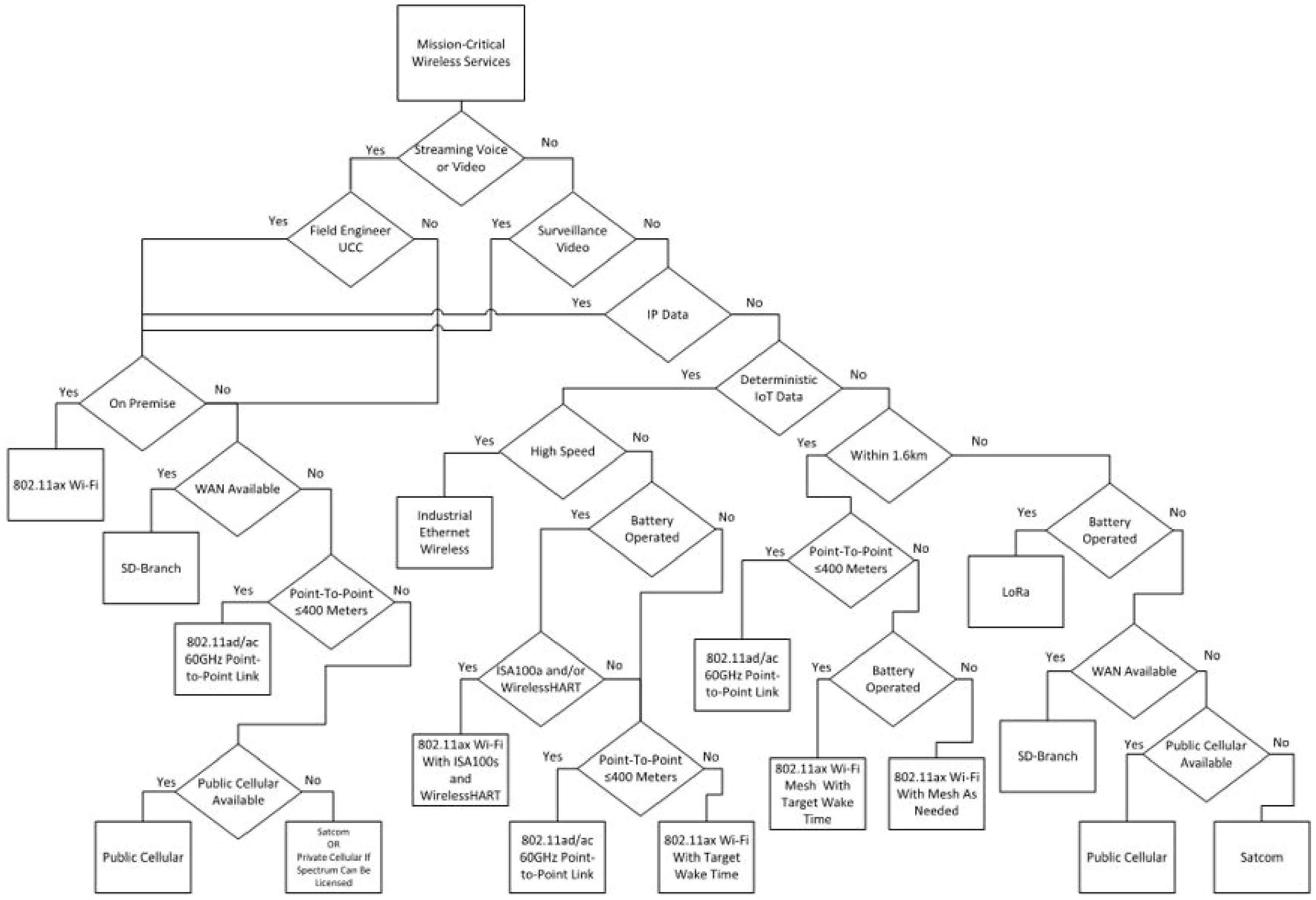
Finally, work is underway to enable cellular infrastructure to operate in unlicensed bands. At this point, the main advantage of licensed spectrum, guaranteed freedom from interference from overlapping transmitters, is left behind. The network becomes similar to a Wi-Fi WLAN and the equipment vendors will need to compete on cost-effective IoT capabilities. In a companion paper on technology we show that Wi-Fi and 4G/5G technology have been converging for some years, and there is no clear technical advantage of one over the other where parameters such as data-rate, spectral efficiency, security, QoS and latency are compared.

When choosing a wireless technology for Industrial IoT, network planners should consider capabilities, cost and also timelines, as many of the features being marketed today will take years to appear in products. For most Industrial IoT networks, company-wide, Wi-Fi will be a universal solution. The emerging 4G and nascent 5G options should be examined, particularly if IoT devices are spread over a wide area or moving at speed: there is opportunity for this technology, but it is not yet proven to the level that Wi-Fi has achieved.

APPENDIX 1: MISSION-CRITICAL SERVICES DECISION TREE

Aruba has developed a decision tree as an aid to network planning for Industrial IoT networks with high-availability requirements.

MISSION-CRITICAL WIRELESS SERVICES DECISION TREE


Mission-Critical Wireless Services
Streaming Voice or Video
Yes
No
Field Engineer UCC
Yes
No
Surveillance Video
Yes
No
IP Data
Yes
No
Deterministic IoT Data
Yes
No
On Premise
Yes
No
802.11ax Wi-Fi
WAN Available
Yes
No
SD-Branch
Point-To-Point ≤400 Meters
Yes
No
802.11ad/ac 60GHz Point-to-Point Link
Public Cellular Available
Yes
No
Public Cellular
Satcom OR Private Cellular If Spectrum Can Be Licensed
High Speed
Yes
No
Industrial Ethernet Wireless
Battery Operated
Yes
No
ISA100a and/or WirelessHART
Yes
No
802.11ax Wi-Fi With ISA100s and WirelessHART
Point-To-Point ≤400 Meters
Yes
No
802.11ad/ac 60GHz Point-to-Point Link
802.11ax Wi-Fi With Target Wake Time
Within 1.6km
Yes
No
Point-To-Point ≤400 Meters
Yes
No
802.11ad/ac 60GHz Point-to-Point Link
Battery Operated
Yes
No
802.11ax Wi-Fi Mesh With Target Wake Time
802.11ax Wi-Fi With Mesh As Needed
Battery Operated
Yes
No
LoRa
WAN Available
Yes
No
SD-Branch
Public Cellular Available
Yes
No
Public Cellular
Satcom

The following notes explain various decision nodes in the tree above:

- Streaming voice or video. Streaming and interactive voice and video have stringent requirements for QoS and are considered a separate category of applications.
- Field engineer UCC. For voice or video, a Unified Communications and Collaboration engineer knowledgeable in QoS techniques should map the end-to-end architecture to ensure QoS requirements (latency, jitter, packet-loss) are met. If an engineer is not available, traffic should be directed to the WAN with the fewest possible intermediate nodes.
- On premise. Wi-Fi should be used for on-premise streaming voice and video in conjunction with the wired LAN. The alternative is to direct traffic to the WAN with the fewest possible intermediate nodes.
- WAN available (x2). If a wide-area private network is available, traffic is directed through that to public network gateways. SD-branch is an Aruba feature that builds a virtual private network between locations over the Internet or dedicated links.
- Public cellular available (x2). If there is no other way to moving traffic off-premise, the cellular network or satellite communications may be available as alternatives.
- Surveillance video. Surveillance video differs from streaming video because it is not used in real-time and does not have restrictions on latency and jitter.
- IP data. While most traffic in an Industrial IoT network will now use the Internet Protocol (IP), many systems use other protocols, often specialized for industrial control.
- Deterministic IoT data. If the data is not IP and must be delivered within specific latency, jitter or error-rate bounds, it needs special consideration.
- High speed. Some deterministic IoT data streams are very-high-speed and should be carried over specialized Industrial Ethernet Wireless links.
- Battery operated (x3). Battery life on Wi-Fi is greatly extended with Wi-Fi 6 through several features including TWT (Target Wait Time).
- ISA100 and/or WirelessHART. These are protocols specifically for Industrial IoT and can be extended over Wi-Fi.
- Within 1.6 km. This distance is feasible with a Wi-Fi mesh network of 2-3 hops from the root node. Beyond that, point-to-point links, normally with Wi-Fi radios, are required to extend the network.

aruba
a Hewlett Packard
Enterprise company

WP_IndustrialIoTina5GworldArch_SK_061220 a00090762enw

Contact Us **Share**