Making higher education institutions smarter with private wireless

How private 4.9G/LTE and 5G technologies can power next-generation campus services and operations

White paper

Higher education institutions are seeking to rapidly digitalize their operations so they can better serve the changing needs of students, academic staff and researchers on their campuses. To succeed, they must evolve their wireless communications infrastructure to offer higher-performing applications and tools that will help their staff and students work more productively. Until now, their main approach has been to upgrade or replace existing Wi-Fi networks, but Wi-Fi technology is starting to show limitations in its ability to meet the increased demands of mobility, latency, throughput and total cost of ownership (TCO).

This paper explores how private wireless networks based on 4.9G/LTE (and eventually 5G) can make it easier and more cost effective for higher education institutions to accelerate their digital transformation and support a wider set of industrial and mission-critical services and operational capabilities. As education terminology is often country specific, we have adopted a language that reflects the nature of the US education system.

Contents

Introduction

Organizations across many industries are accelerating the digitalization of a wide range of services and applications so that they can access and control them remotely. Higher education institutions also have a growing need to digitalize their services and operations on and off campus. To succeed with digitalization, these institutions must evolve their wireless communications infrastructure so that they can offer high-performing services that will help their students, academic staff, researchers and operations teams work more productively.

Until now, higher education institutions have focused on complementing fixed Ethernet infrastructure by upgrading or expanding existing campus Wi-Fi networks. But Wi-Fi technology is starting to show limitations in its ability to support some of the new services and operational applications that institutions want to roll out. These limitations extend to reliability, security, predictable performance, coverage, multi-user capacity and mobility, all of which are required for day-to-day communication and new business- or mission-critical operational broadband and Internet of Things (IoT) applications.

Fortunately, governments in some countries have enabled alternative – and more appropriate – paths to the deployment of state-of-the-art communication technologies. In the US, for example, the Federal Communications Commission (FCC) recently authorized full commercialization of OnGo services using the 3.5 GHz CBRS band. This authorization means that higher education institutions now have access to 4.9G/LTE and 5G technology options without having to acquire a spectrum license. As such, they can integrate true mobile broadband access within their operations to benefit students, faculty and staff. The fact that these network technologies and architectures are based on international 3GPP standards makes investing in them future safe.

LTE and 5G are available in configurations that are perfectly suited for offering broadband services as well as for building industrial-grade IoT private wireless networks that can support new Industry 4.0 applications. These 3GPP technologies bring the best features of wireless, Ethernet and cable connectivity (including CAT cabling and fieldbus) and have proven their capabilities in large consumer mobile networks and industry verticals.

Another factor is the recent adaptation of LTE and 5G network designs and architecture to cost competitively support private enterprise and campus network deployments and use cases. A private wireless network does not have the same requirements as a public LTE network, which may need to cover a large geographical area and provide service to hundreds of thousands of devices at the same time. Using the same technology as public networks, however, these private networks can scale from a few hundred connections on a single small cell to tens of thousands on a macro antenna.

Private wireless networks based on LTE or 5G can enable higher education institutions to fulfill their diverse and evolving connectivity needs while leveraging their existing fiber, Ethernet and Wi-Fi network infrastructure. LTE and 5G are true general-purpose wireless communication technologies. They allow institutions to support a wide range of use cases and requirements from their many stakeholders and end users, as described in the next section of this paper. Private LTE networks are the main option for higher education institutions today and provide a gateway to tomorrow's 5G networks. Networks that use Nokia 4.9G/LTE technology offer the fastest route to 5G.

To keep pace with new demands and get the most from their networks, higher education institutions should design and deploy a holistic and integrated wireless infrastructure solution that includes Wi-Fi, private 4.9G/LTE and/or public LTE. Each of these wireless solutions provides capabilities and value for specific use cases and applications. They can be viewed as complementary, rather than competing, solutions.

As they plan future wireless deployments, higher education institutions should look at which technology is best suited to support each of the use cases and services they plan to roll out. To derive maximum benefit from Industry 4.0 and the smart IoT revolution, they should also be sure to choose technologies that their peers and enterprise partners will use for digital transformation.

A growing need for wireless communications

Higher education institutions have diverse needs that require campus-wide communications. The main use cases that are driving their requirements for new broadband wireless connectivity include:

- Classroom technologies: Equipping classrooms and auditoriums with services such as smart boards, smart podiums or smart lighting.
- Digital productivity tools: Providing staff and students with access to office productivity tools on their mobile devices, and providing broadband access to students attending courses and practicums.
- Industry 4.0 labs: Enabling labs to study and research Industry 4.0 technologies using communication technology that will be deployed for business- and mission-critical IoT applications across many industries.
- Campus utilities: Optimizing building, water, power and environmental management with building automation and control systems and data from IoT sensors. Reliable broadband coverage and connectivity can also help institutions develop new campus-wide logistics systems using automated guided vehicles (AGVs).
- Campus security: Easing the deployment of surveillance cameras, smoke sensors and emergency call buttons across the campus. Broadband wireless connectivity can also open the door to video analytics use cases such as drone- or robot-based surveillance or automated fever detection based on data from thermal cameras.
- On-campus communications: Keeping academic and operations staff connected with VoIP/PBX phone systems and group communication applications such as push-to-talk (PTT) and push-to-video (PTV).
- Digital signage: Using connected digital billboards to spread general information, provide emergency announcements, help with wayfinding, engage visitors and make campus life simpler.
- Remote learning: Providing augmented and virtual reality (AR/VR) classrooms that can be accessed from anywhere in the world. This capability allows teachers or classrooms to be located on or off campus.
- Residential student housing connectivity: Providing students with good and affordable high-speed internet access, facility management services and emergency calling. The network can also support home automation and smart devices, including smart speakers, doorbells and locks.
- Mobile e-commerce: Providing secure point-of-sale terminals throughout the campus to support ticket sales, food and beverage services, concerts and events. These capabilities can be complemented with drone- or autonomous vehicle-based delivery services.

Comparing private wireless to other typical network technologies

Most enterprises and higher education institutions value the benefits of wireless and mobile technologies. They also recognize that these technologies can provide pervasive connectivity, flexibility, ease of use and the ability to connect anything, even inside machines. However, they tend to believe that the high levels of service quality, reliability and security required for business-critical communications can be achieved only with hardwired solutions such as fiber or Ethernet CAT cables.

Figure 1. The different levels of criticality in enterprise networking and the capabilities of the two main wireless networking technologies compared.

Increasing need for network reliability, predictability, security and performance

Level of criticality	Day-to-day	Business-critical	Mission-critical
Communication needs	Public and business	Business and operations	Operations
Business drivers	High-speed broadband, voice and video comms, business applications	Ubiquitous, reliable and secure connectivity, mobility	Lives at risk, potential for environmental disaster.
Typical applications	Working, learning, social, information and entertainment, etc.	Process control, telemetry, automation, digital innovation, etc.	Real-time control systems, first responder, power grid control, autonomous vehicles, etc.
Where used?	Home, office, city hotspots, trains and stations, passenger terminals, etc.	Factories, rail and airport operations, **higher education campuses**, etc.	Utilities, rail and air control, mining, oil & gas, public safety, etc.
Network technology	Wi-Fi		
	4G/LTE and 5G cellular wireless		

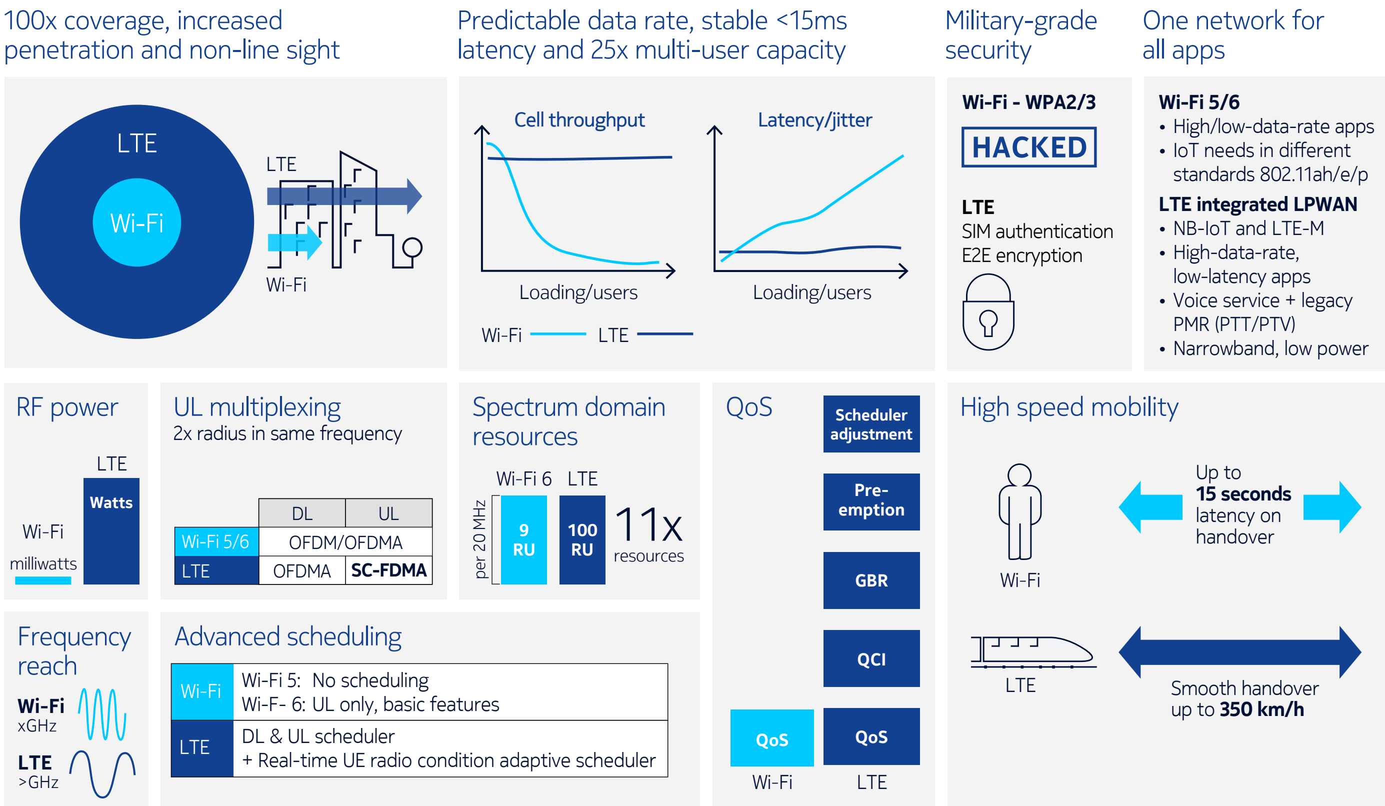
Secure and contained cable environments, such as those based on CAT cables or fiber strands, are hard to beat in terms of reliability and security. These environments will continue to be used for many fixed assets in industrial and higher education campuses.

Nonetheless, 4.9G/LTE and 5G are similarly reliable, predictable and secure, and offer many advantages by supporting both wireless and mobile communications. These technologies are based on 3GPP standards and have been proven in public networks. Compared to Wi-Fi, 4.9G/LTE provides much more predictable performance relative to latency and data rate. It also provides high multi-user capacity and can connect hundreds of devices, machines, sensors or workers with each access point, referred to a base transceiver station (BTS) or eNodeB in cellular terminology. These capabilities can support a very high density of devices in the same area.

Enterprises that have tried using IT-based wireless technologies such as Wi-Fi, mesh Wi-Fi or Bluetooth for operational critical connectivity have rapidly realized their limitations. These technologies are perfectly suited for office-type communications and will continue to be used for these applications. But they were not designed to meet the performance demands of business-critical communications.

Figure 2 highlights some of the key advantages of choosing LTE over Wi-Fi for business-critical applications.

Figure 2. Business-critical capabilities of LTE versus Wi-Fi.



The following sections compare 4.9G/LTE with Wi-Fi in relation to six capabilities that are important to higher education institutions. To ensure that the comparison is as neutral as possible, all the diagrams presented below compare MulteFire to Wi-Fi 802.11ac in the same laboratory conditions. MulteFire is a technology, similar to CBRS, that allows deployment of LTE in the unlicensed or shared 5.x GHz spectrum and that can coexist with other wireless/Wi-Fi networks.

In countries like the US, where CBRS is available, higher education institutions can expect higher performance from CBRS OnGo Band 48 spectrum compared to MulteFire spectrum or LTE in licensed spectrum (communication service provider-leased spectrum, vertical spectrum and lightly licensed spectrum) because it provides better overall performance in terms of coverage, capacity, reliability, latency and predictability. Unlike Wi-Fi, LTE performance remains stable as the number of connections increases.

Security

Higher education institutions have identified cybersecurity as a high-priority requirement for wireless technology deployments. Many cite security concerns as a reason why they have not moved applications or use cases to a wireless solution in the past.

In contrast to Wi-Fi, which lacks strong security and is vulnerable to hackers, the 3GPP standard requires end-to-end encryption with strong cyphering algorithms for the air interface and IPsec for communication between network elements. It also requires that all users and objects be securely authenticated using SIM cards or embedded SIM (eSIM). To date, LTE network security has never been compromised. Stringent testing by public agencies for public safety use has not shown any major vulnerabilities with LTE, and cybersecurity has been strengthened for 5G.

High reliability

One key difference between Wi-Fi and LTE is in the way they handle interference. LTE has several mechanisms for dealing with interference. These include a scheduler that prioritizes resources in frequency and time domains every millisecond to maximize radio efficiency. There are also mechanisms that constantly monitor the radio condition of each device and adapt the encoding and resource usage. For example, these mechanisms may allocate less "noisy" sub-frequency blocks to improve the chance of getting data through the first time. They may also improve the encoding rate to get more data through.

The way Wi-Fi avoids interference means that frequency is only available when other devices are finished using it, which makes latency unpredictable on a congested link. The Wi-Fi 6 standard introduces a concept like a scheduler but it offers less advanced capabilities than those provided by LTE today.

LTE networks are based on carrier-grade communications systems and architectures. They have already proven their worth in the public space. Today, a well-designed LTE network in a city would provide three nines reliability, or 99.9 percent uptime. Nokia has observed that a private LTE network with a dedicated BTS and core deployed on premises can reach four nines reliability, or 99.99 percent uptime.

Private LTE networks provide higher performance because users have capacity dedicated to them rather than having to share it, because there is much less fluctuation in the loads and number of connected users, and because the enterprise controls network element interconnections from end to end. Private LTE networks also support several techniques (e.g., scheduler parameters) and possible improvements (e.g., dual connectivity) that can be used to offer up to five nines reliability (99.999 percent uptime, or five minutes of downtime per year) for a specified set of high-priority users.

Large outdoor and pervasive indoor coverage

Pervasive coverage is critical on industrial or higher education institution campuses. But these campuses often have environments that feature potential obstructions to coverage, such as foliage, large vehicles, protective metal fences, buildings and containers.

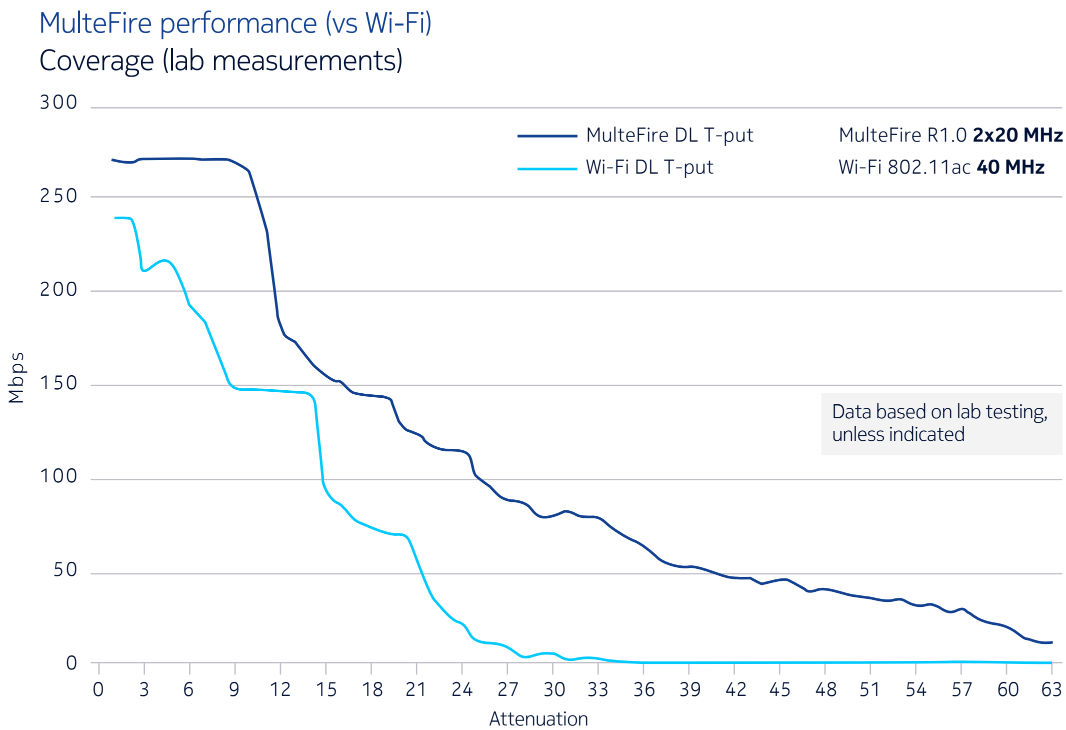
Wi-Fi has no special features to overcome coverage issues. The only solution is to deploy more access points. LTE, in contrast, has an extensive arsenal of tools for overcoming challenging coverage issues in dense urban centers with high buildings, as well as indoor environments such as classrooms, stadiums, dorm rooms and shopping concourses. In comparison to these environments, most industrial and higher education campuses do not pose a challenge for LTE. It is more than capable of connecting all machines, sensors (sometimes within machines), workers and vehicles.

LTE can operate in licensed spectrum from a public mobile operator or use licensed or unlicensed spectrum designated for vertical use, such as for a higher education institution. Licensed spectrum brings some added benefits. For example, it comes in frequencies below 2 GHz, which offers increased coverage because of the physical properties of these longer radio waves. It also allows emission of radio frequency (RF) signals at higher power. This means that it takes a much smaller number of LTE cells than Wi-Fi access points to provide connectivity outdoors or in a high-ceiling environment such as those that feature in most university campuses or auditoriums.

The gains can vary significantly when LTE replaces Wi-Fi. Nokia has observed cases where 150-plus outdoor Wi-Fi access points were replaced by 10 micro BTS small cells in an open environment. The results were improved coverage inside key buildings within the campus and extended coverage to a much wider area around the campus. The new cells also provided enough coverage to support future expansion of the campus footprint.

The device uplink radio is often the limiting factor for coverage because individual devices cannot emit as much power as the access point radios. Unlike Wi-Fi, the 3GPP standards for LTE specify a different modulation technique (SC-FDMA instead of OFDM) for the uplink, which provides a significant coverage gain. This means that even if the same frequency and output power are used for LTE (as in the case of MulteFire), the coverage gain is about twice the coverage radius, making for much larger cells. Use of CBRS Band 48 expands the coverage radius even further.

Figure 3. Coverage performance of Wi-Fi versus LTE for the same frequency and power output.

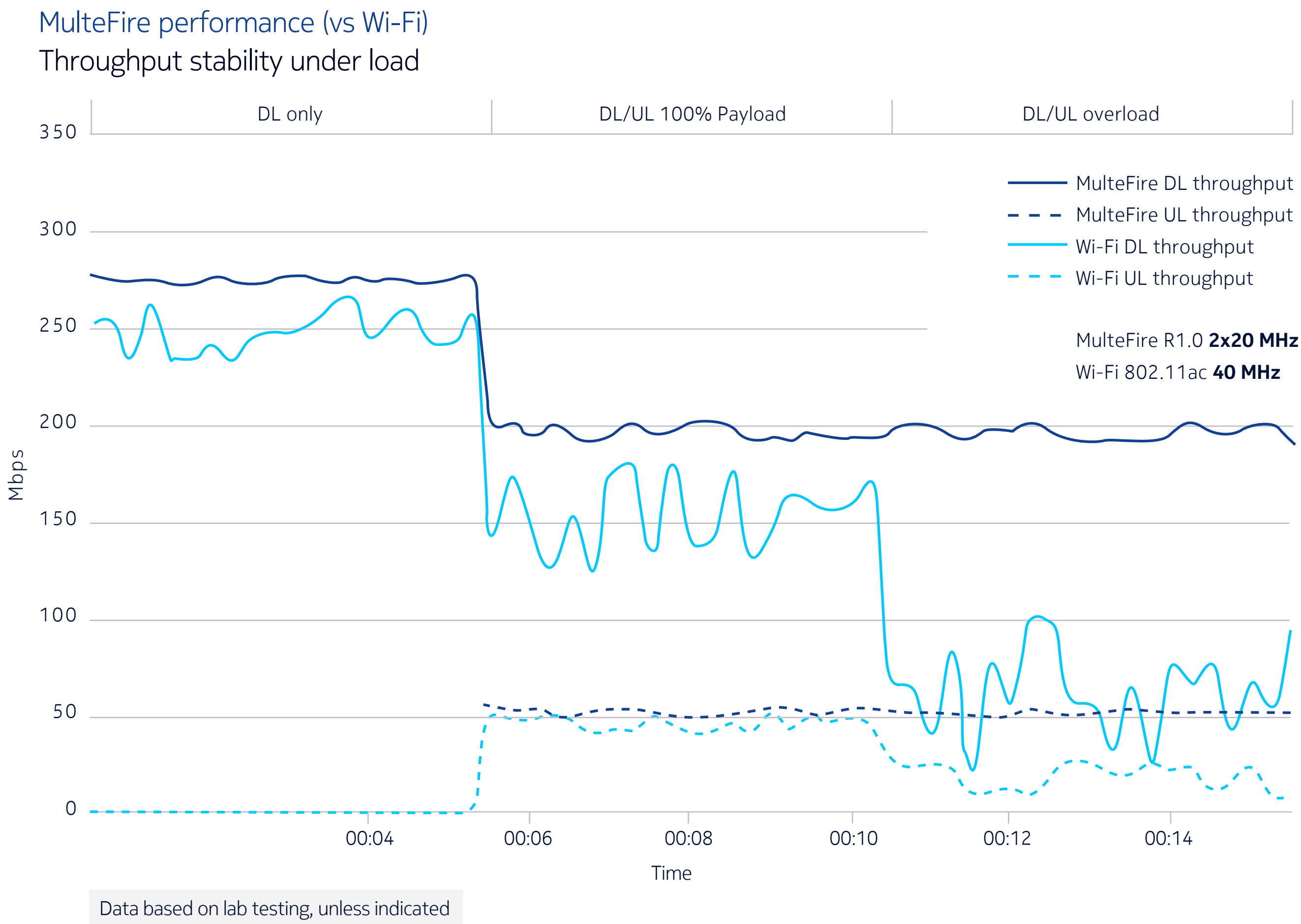


Predictable performance (data rate and latency)

With a locally deployed core or an edge cloud server running applications on premises, private LTE networks provide much better end-to-end latency than public networks. This is because information travels very short distances to reach the core or edge cloud. The typical latency of private LTE networks is 9–15 ms, compared to 20–80 ms for public LTE networks. With additional scheduler adjustments, quality of service (QoS) settings and preemptive uplink grants, the end-to-end latency can be maintained at around 10 ms for certain devices. Future standard releases of LTE will take baseline end-to-end latency from 8 ms to 4 ms and then to 2ms. 5G will take latency to less than 1 ms.

As discussed above, one of the key differences between current-generation Wi-Fi 5 and LTE is the scheduler. A Wi-Fi network may sometimes have a higher peak performance than LTE if there are only a few users per access point and no interference conditions. However, Wi-Fi performance degrades rapidly when more users are connecting and transmitting data, or in interference-prone environments. In comparative testing, we have seen Wi-Fi latency jump to more than two seconds, and sector throughput (i.e., the combined performance of all users) drop by as much as 90–95 percent, when the network is congested. In contrast, the LTE scheduler maximizes spectral resource use, and therefore the radio link, based on individual user radio conditions. As a result, the LTE sector throughput remains stable (i.e., it provides predictable capacity) and the latency can be maintained even with heavy loading.

Figure 4. Comparison of throughput stability under load for LTE (MulteFire) versus Wi-Fi.



The Wi-Fi 6 standard introduces the possibility of adding a scheduler on the uplink (UL) but not on the downlink (DL). The number of bandwidth resource blocks per MHz is much lower and the resource allocation and encoding mechanisms are not as advanced. This means spectral efficiency is lower, which equates to lower bandwidth. As of today, most Wi-Fi 6 solutions do not implement this UL scheduler, and it remains to be seen when this will occur. The implementation of a scheduler will have a significant cost impact on Wi-Fi access points because it will increase microprocessor without interlocked pipelined stages (MIPS) requirements and code complexity. Vendors may initially be reluctant to implement such a scheduler because of the risk of becoming uncompetitive.

High multi-user capacity

The LTE scheduler also plays a key role in enabling high multi-user capacity by supporting several hundred devices per LTE BTS. For example, the Nokia Flexi Zone small cell BTS, known for its macro capacity, can handle up to 800 actively communicating users per small cell, with thousands more connected to it. Wi-Fi uses round-robin allocations, and its performance crumbles when more than 30–50 devices are actively communicating. As IoT sensor use tends to multiply in a full-blown Industry 4.0 implementation, it will be critical to have the additional headroom that LTE can provide.

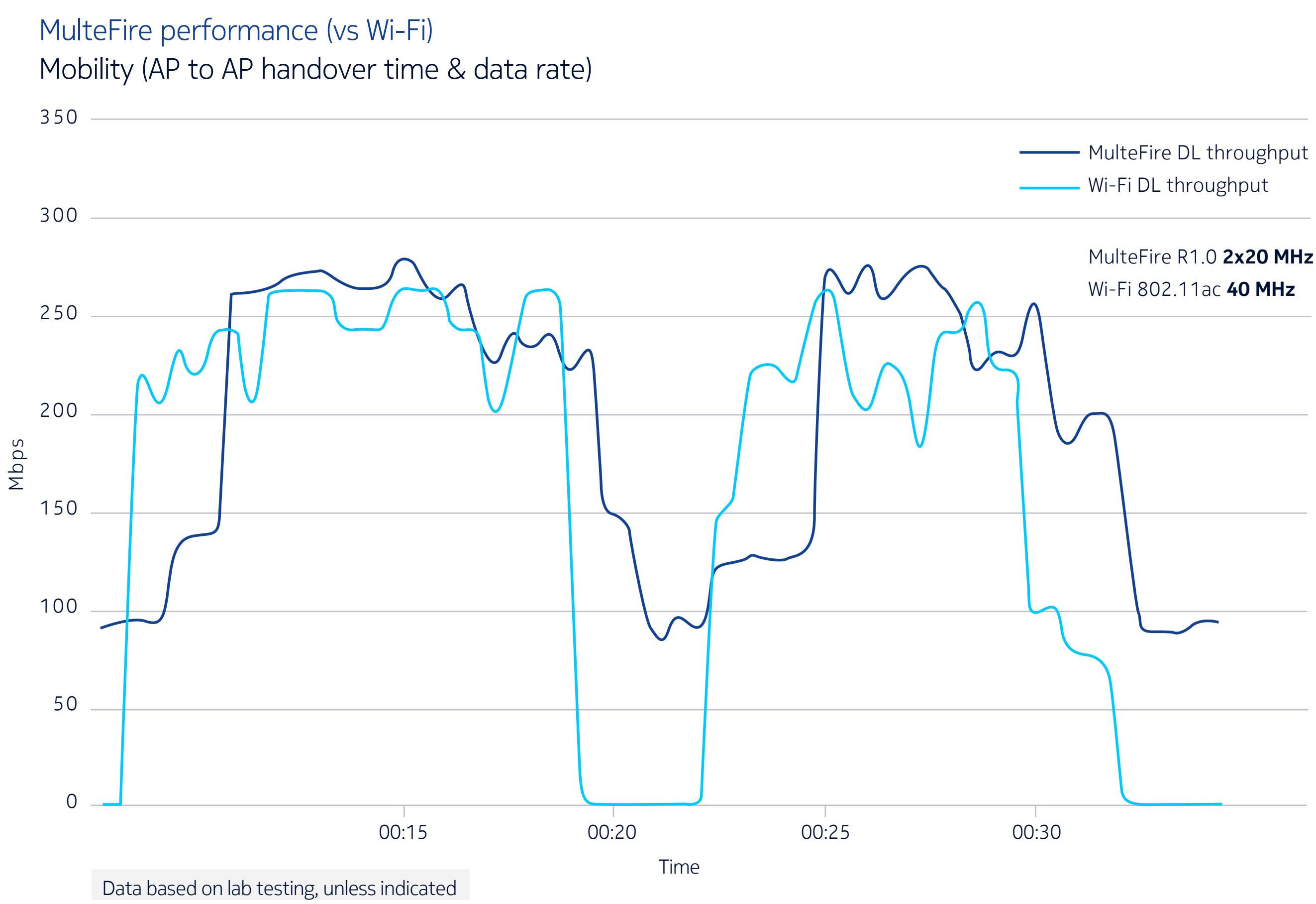
Full mobility

Wi-Fi is part of the IEEE 802 set of LAN protocols. Its initial design intent was to connect computers in homes and offices where only limited mobility was imagined. In contrast, LTE comes from 3GPP mobile radio standards with a key requirement for mobility. This requirement includes vehicular speed up to 350 km/h, which will enable the network to maintain live LTE connections for high-speed trains such as those found in France, China and Japan. The big difference is that mobility with Wi-Fi is mostly device driven and varies from one device to another. Mobility on 3GPP is a coordinated action between the device that detects and reports on its environment and the network core elements that analyze this data to look at all possible handover candidates and coordinate the handover with the target mobility BTS and the devices.

The mobility feature of 3GPP wireless technologies is particularly useful for industries that have large campuses with combined indoor and outdoor spaces. Many of these industries rely on different kinds of vehicles, including some that move at higher speeds, such as driverless buses, elevators and drones. The ability to maintain connectivity during handovers between radios is critical. This is a weakness in the Wi-Fi standard. Dropped connections can lead to software and data transmission problems that cause Wi-Fi-connected vehicles to crash.

In lab testing, we have observed disconnection–reconnection times of up to 15 seconds for Wi-Fi networks. In real life, we have seen factory AGVs suffer from repeated failures as they pass from one Wi-Fi access point to another. Changing the communication system to LTE or 5G quickly fixed these systematic failures.

Figure 5. Measuring mobility and handover times for LTE (MulteFire) versus Wi-Fi.



One wireless network for all applications

Higher education institutions can simplify their operations and significantly reduce cost by moving from multiple application-specific networks to a single network that handles all types of loads. A private 4.9G/LTE network offers better capabilities and performance than any other type of wireless network and will support a smooth evolution to future 5G network technologies. It can tackle all types of traffic while offering plenty of capacity and room to grow.

In addition to supporting high-data-rate, low-latency applications, LTE release 13 standards specify new IoT protocols (LTE-M and NB-IoT) that are particularly well suited for sensor-type devices. These protocols offer reduced complexity, optimized power consumption and lower data rates (LTE-M supports applications up to 1 Mbps and NB-IoT to 200 Kbps). Modems that use these protocols can run several years on battery power alone. These capabilities make it simple to deploy sensors in campuses or inside machines. LTE-M and NB-IoT operate with the same LTE network and equipment. Supporting them is a baseline capability of the Nokia industrial-grade private wireless solution.

When we deploy private LTE networks on campuses, we often find that enterprises or institutions have private mobile radio (PMR) or digital mobile radio (DMR) communication systems, such as TETRA or P25, that would need to interconnect and interoperate with LTE. Nowadays, these services can be implemented as group communication applications, such PTT and PTV, that run on top of LTE (and eventually 5G). They advantageously replace aging private radio systems and add new functionalities.

Total cost of ownership

The benefits of private wireless networks that can connect many things, machines and people are obvious. But how do these networks compare to CAT cabling or Wi-Fi alternatives with respect to TCO?

Given the multitude of IoT sensors and machine-based devices to connect in most Industry 4.0 implementations, traditional LANs will require a significant investment in cabling and switches. This will lead to more complex LAN architectures. Although each LTE BTS will require an Ethernet or microwave backhaul connection, it will be able to scale easily and connect thousands of workers, machines and sensors. This will greatly reduce the cost per endpoint.

Wi-Fi is often seen as a very cost-effective solution. Its combination of low cost and simplicity is its strength in IT-like applications. To compare the TCO of a private LTE system to that of a Wi-Fi system, we need to consider four key differences and factors at a network/system and performance level.

- An LTE BTS (or small cell) is more expensive than a Wi-Fi access point. The higher-powered radios and scheduler capabilities of LTE BTSs account for much of this cost difference. As described above, these capabilities are part of what makes LTE much better than Wi-Fi at addressing the critical application requirements of higher education institution campus users. The higher-powered radios in an LTE BTS are one of the reasons LTE provides much better coverage than Wi-Fi. For any given site area, an institution will require five to ten times fewer LTE BTSs than Wi-Fi access points. This will offset the increased cost per small cell by lowering installation and maintenance costs.
- LTE requires a core and Wi-Fi does not, except for management and user authentication. LTE also requires coordination between the BTS and other features that operate centrally. The core enables device mobility, coordination for multi-cell deployments, better interference management, QoS differentiation and improved security and availability. Thanks to function virtualization, LTE core solutions have been adapted to suit the smaller deployments required in higher education institution campuses. For example, one Nokia private LTE core solution can operate the seven or eight functions required for private LTE on a mini PC-sized server.

- LTE needs SIM cards or eSIM to authenticate users. It strictly controls who has access to the network and provides much greater security than Wi-Fi. Most Wi-Fi hacking techniques rely on breaking the authentication methods used in a given network.
- LTE networks are often seen as more complex to operate and manage. The Nokia private wireless solution makes the best use of self-organizing network (SON) features to ease deployment and optimization, while featuring an easy-to-use management portal. In other words, higher education institutions can avoid the complexity associated with LTE if they want to. Institutions can also take advantage of the full capabilities of our operations and management system if they want the ability to adjust parameters to maximize network capabilities and performance in the future.

With so many parameters to account for, including frequency, site size, indoor and/or outdoor deployment and number of users, it is difficult to provide a generic answer about how TCO compares between private LTE and Wi-Fi systems. Our experience shows that similar-sized private LTE and dedicated Wi-Fi campus networks that reliably support the same critical wireless applications and number of connections over the same coverage area have a comparable TCO.

The two big pluses for LTE are that it has a much larger coverage area, which lowers the initial CAPEX and installation cost, and that it has much higher capacity in terms of active devices, which reduces the need for future investment to scale the network. These two factors tend to compensate for the extra cost of the LTE radios and the need for a core network. LTE offers additional savings by reducing the complexity of the LAN infrastructure and providing more flexibility wherever it replaces CAT cabling. In addition, LTE can often replace aging PMR and DMR networks, and it can offload existing IT Wi-Fi networks so that they operate more efficiently.

Conclusion

New and evolving demands are enabling higher education institutions to digitalize the tools and services they provide on their campuses. To make a quick and successful digital transformation, these institutions will need wireless solutions that can overcome the capacity, coverage and feature limitations of their existing Wi-Fi networks. These networks are well suited for day-to-day business communications but are not optimized for business- or mission-critical communications.

Private 4.9G/LTE (and future 5G) networks offer a solution to this challenge. These networks enable higher education institutions to leverage 3GPP technologies and new spectrum options to provide the security, reliability, coverage, mobility, capacity and flexibility that digital and Industry 4.0 applications demand. By complementing Wi-Fi with private 4.9G/LTE networks, they can power a new generation of campus services that will address the changing needs of staff and students while reducing network TCO.

Abbreviations

3GPP	3rd Generation Partnership Project
AGV	automated guided vehicle
AR	augmented reality
BTS	base transceiver station
CBRS	Citizens Broadband Radio Service
DL	downlink

DMR	digital mobile radio
eSIM	embedded SIM
FCC	Federal Communications Commission
GBR	guaranteed bitrate
IoT	Internet of Things
LAN	local area network
LMR	land mobile radio
LTE	Long Term Evolution
LTE-M	LTE-Machine Type Communication
MIPS	microprocessor without interlocked pipelined stages
NB-IoT	Narrowband IoT
OFDM	orthogonal frequency-division multiplexing
OFDMA	orthogonal frequency-division multiple access
PMR	private mobile radio
PTT	push to talk
PTV	push to video
QCI	QoS class identifier
QoS	quality of service
RF	radio frequency
SC-FDMA	single-carrier frequency-division multiple access
SIM	subscriber identity module
TCO	total cost of ownership
UL	uplink
VR	virtual reality

CONTACT RFS

About Nokia

We create technology that helps the world act together.

As a trusted partner for critical networks, we are committed to innovation and technology leadership across mobile, fixed and cloud networks. We create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Adhering to the highest standards of integrity and security, we help build the capabilities needed for a more productive, sustainable and inclusive world.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: 1404101272045719718 (August) CID205506