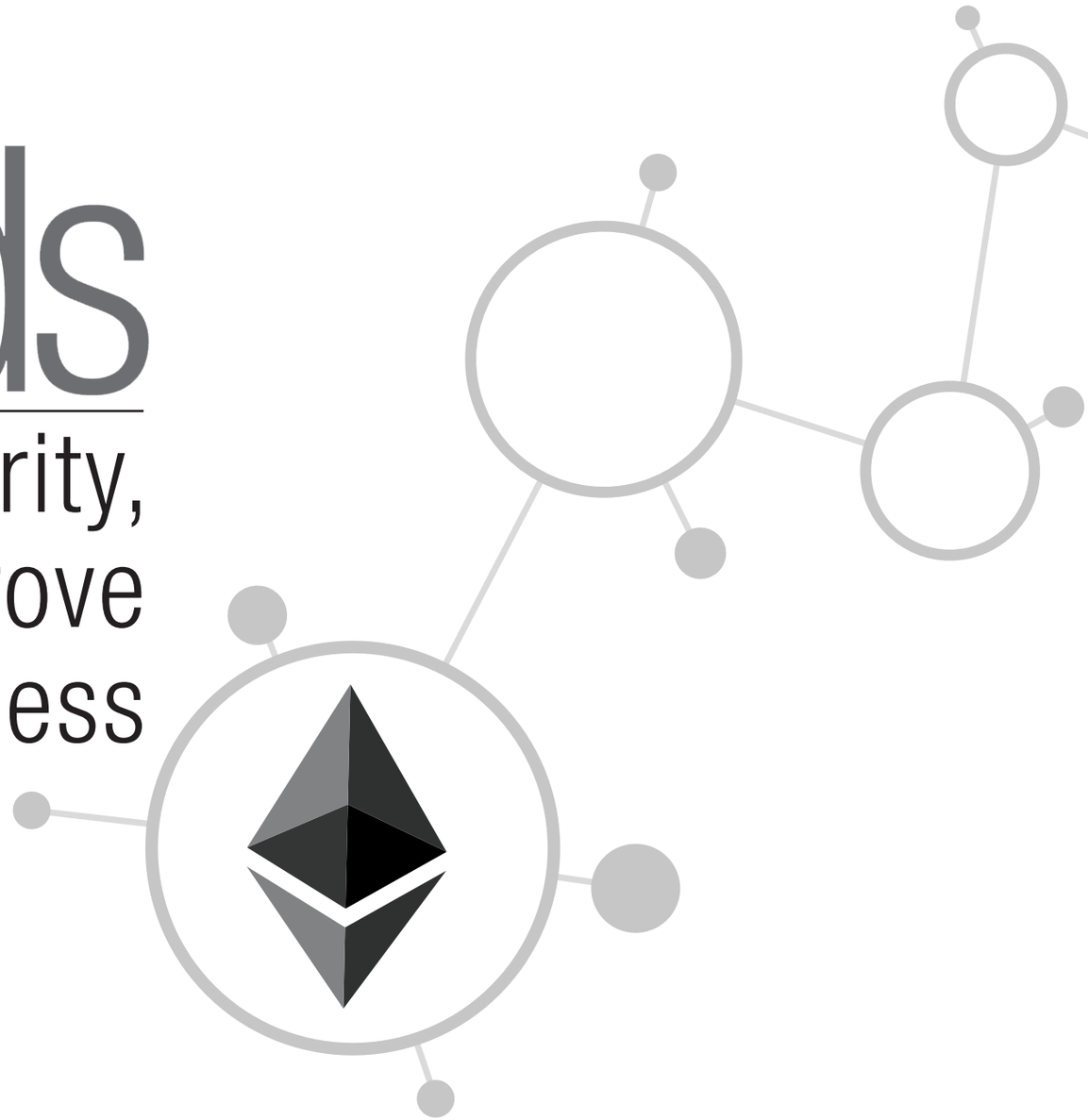
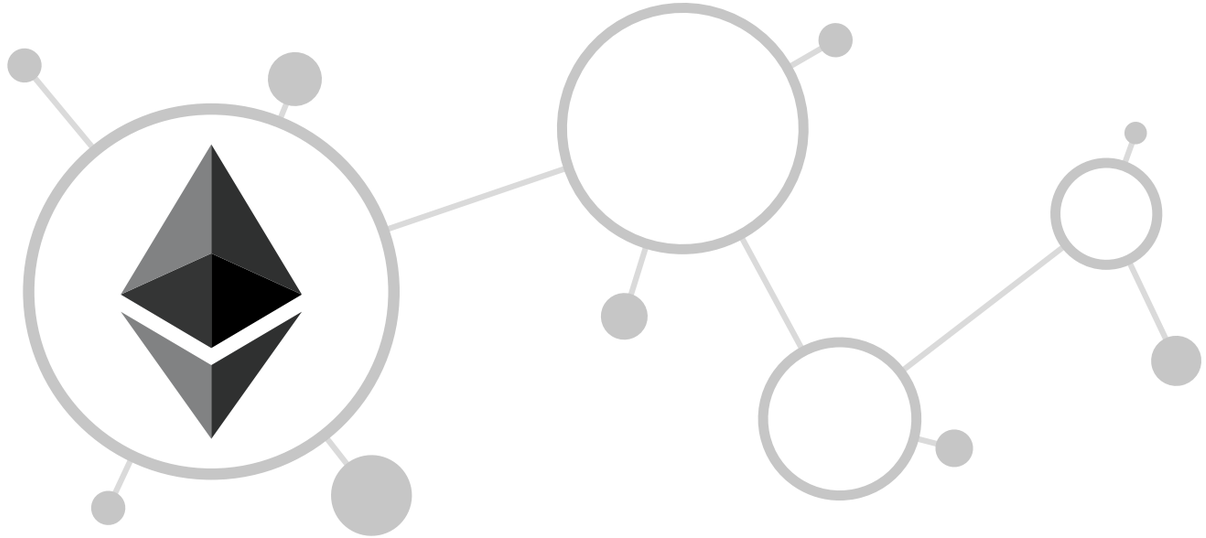
Must reads

Requirements, Security, and Solutions to Improve Next-Gen Wireless



Sponsored by ROHDE&SCHWARZ
Make ideas real

Requirements, Security, and Solutions to Improve Next-Gen Wireless



INSIDE

Telecoms, Wireless, and Adjacent Technologies in 2030

By Dean Bubley, *Technology Analyst and Founder, Disruptive Analysis*

Here's my look into five to 10 years out to consider what telecoms, wireless, and related technologies will look like in 2030. A decade from now, we could see things like power-shaming indicators, bonded 5G/6G and Wi-Fi 9, multi-network software-defined connectivity, contextual communications in IoT devices, and Alexa bots.

If you read my articles and tweets, you probably know what I think about 2020 already. Private cellular networks will be important (4G, initially). 5G fixed wireless is interesting and will grow the FWA

market — but it won't replace fiber. 5G is "just another G" and is overhyped, especially until the new core matures.

So, at the start of the 2020s, what about the next decade? Assuming I haven't retired to my palatial Mars-orbiting private moon in 10 years' time, what do I think I'll be writing, podcasting, or neural-transmitting about in 2030?

Let's have a few shots at this more distant target:

- **6G:** In 2030, the first 6G networks are already gaining traction in the marketplace. The first users are still fixed connections to homes and personal devices that look similar to phones and wearables but with a variety of new display and UI technologies, including contact lenses and advanced audio/haptic interfaces. 6G represents the maturing of various 5G concepts (such as the new core), plus greater intelligence to allow efficient operation.

- **Details, details:** Much of the 2020s will have been spent dealing with numerous back-office problems that have stopped many early 5G visions from becoming real. Network slicing will have thrown up huge operationalization and security issues. Dealing with QoS/slice roaming or handoff at borders between networks (outdoor/indoor/private/neutral/international) will be hugely complex. Edge computing scenarios will turn out to need local peering or interconnection points. All of these will have huge extra complexities with billing, pricing, and monitoring. mmWave planning and design tools will need to have matured, as well as the processes for installation and operation.

- **Device-network cooperation:** By 2030, mobile ecosystems and control software will break today's silos between radio networks, devices, and applications much more effectively. Sensors in users' devices, cell towers, and elsewhere will be linked to artificial intelligence, which works out how, why, and where people or internet of things objects need connectivity and how best to deliver it: Recognize a moving truck with machine vision and bounce signals off of it opportunistically. Work out that someone is approaching the front of a building and pre-emptively look for Wi-Fi, or negotiate with the in-building neutral host on a marketplace before they enter the door. Spot behavioral patterns such as driving the same route to work and optimize connectivity accordingly. Recognize a low battery and tweak the "best connected" algorithm for power efficiency and downrate apps' energy demand. There will be thousands of ways to improve operations if networks stop thinking of a "terminal" as just an endpoint and look for external sources of operational data — that's a 20th century approach. Expect Google's work on its

Fi MVNO & Android/Pixel phones, and similar efforts by Samsung and maybe Apple, Qualcomm and Arm, to have driven much of this cross-domain evolution.

- **Energy-aware networks:** Far more energy awareness will be designed into all aspects of the network, cloud, and device/app ecosystem: how best to optimize wired/wireless data for power demand, where best to charge devices, "scavenge" for power, and maybe even "nudge" people to lower-energy applications or consumption behaviors by including "power shaming" indicators. If 3GPP and governments get their act together, as well as vendors, overall 6G energy use will be a higher-priority design goal than throughput speed and latency.

- **Wi-Fi:** We'll probably be on Wi-Fi 9 by 2030. It will continue to dominate connectivity inside buildings, especially homes and business premises with FTTX broadband. It will continue to be used for primary connectivity on high-throughput/low-margin/low-mobility devices like TVs and display screens, PC-type devices, AR/VR headsets, and so on. It will be bonded together with 5G/6G and other technologies with ever-better multi-path mechanisms, including ad hoc device meshes. Fairly little public Wi-Fi will be delivered by "service providers" as we think of them today. We'll probably still have to suffer the "6G will kill Wi-Fi" pundit pieces and hype, though.

- **Spectrum:** The spectrum world changes slowly at a global level, thanks to the glacial four-year cycle of ITU WRCs. By 2030, we will have had 2023 and 2027 conferences, which will probably harmonize more spectrum for 5G/6G, satellites and high-altitude platforms (HAPS), and Wi-Fi–type unlicensed use. The more interesting developments will occur at national/regional levels, below the ITU's role, in how these bands actually get released/authorized — and especially whether that's for localized or shared usage suitable for private networks and other innovators. I think we'll be closer to some of the "spectrum as a service" models and marketplaces I've been discussing over the last two years, with more fluid resale and temporary usage permits. International allocations will still differ though. We will also see much more opportunism and flexibility in band support in silicon/devices, as well as more sophisticated approaches to in-band sharing between different technologies. I'm less certain whether we will have progressed much with commercialization of mmWave bands 20–100 GHz, especially for mobile and indoor use.

- **Private/neutral cellular:** Today, there are about 1,000 mobile network operators (MNOs) globally (public and private). By 2030, I'd expect there to be between 100,000 and 1 million networks, probably with various new types of service providers, aggregation hubs, and consortia. These will span industrial, city, office, rural, utility, "public venue," and many other domains. It will be increasingly hard to distinguish private from public, e.g., with MNOs' campus networks with private cores and hybrid public/private spectrum. Some networks will look like micro-telcos (e.g. an airport providing access to caterers and airlines) and will need billing, management, and security tools — and perhaps new forms of regulation.

- **Security & privacy:** Both good and bad guys will be armed to the teeth with AI. We'll see networks attacked physically as well as logically. We'll see sophisticated theft of credentials and what we quaintly term "secrets" today. There will be cameras and mics everywhere. Quantum threats may compromise encryption — and other quantum tools may enhance it, as well as provide new forms of identity and authentication. We will need to be wary of threats within core networks, especially where orchestration and oversight is automated. I think we will be wise to avoid "monocultures" of technologies at various levels of the network — we need to trade off efficiency and scale versus resilience.

- **Satellite/HAPS:** We'll definitely have more satellite constellations by 2030, including some huge ones from SpaceX or others. I have my doubts that they will be "game changers" in terms of our overall broadband use, except in rural/remote areas. They won't have the capacity of terrestrial networks, and signals will struggle with indoor penetration and uplink from anything battery-powered. Vehicles, planes, boats, and remote IoT will be much-better-connected, though. Space junk and cascading-collision scenarios like the movie "Gravity" will be a worry, though. I'm not sure about drones and balloons as HAPS for mass-market use, although I suspect they'll have some cool applications we don't know about today.

- **Cloud & edge:** The bulk of the world's computing cycles and data storage will continue to occur in massive data centers (perhaps heading toward a terawatt of aggregate power by 2030) and on devices themselves, or nearby gateways. But there will be a thriving mid-market of different sorts of "edge." This will partly be about low latency, but not as much as most people think. It will be more about saving mass data-transport costs, protecting "data sovereignty," and perhaps optimizing energy consumption.

There will be a lot of value in the overall orchestration of compute tasks for applications between multiple locations in the ecosystem, from chip-level to hyper-scale and back again. The fundamental physical quantum of much edge compute will be mundane: a 40-foot shipping container, plonked down near sources of power and fiber.

- **Multi-network:** We should expect all connectivity to be "software defined" and "multi-network." Devices will have lots of radios, connecting simultaneously, with different paths and providers (and multiple eSIM/other identities). Buildings will have multiple fibers, wireless connections, and management tools. Device-to-device connections and relaying will be prevalent. IoT will use a selection of LPWAN technologies as well as Wi-Fi, cellular, and short-range connections. Satellite and maybe Li-Fi (light-based) connections will play new roles. Arbitrage, bonding, and load balancing will occur at multiple levels, from silicon to OS to gateway to mid-network. Very few things will be locked to a single network or provider — unless it has unique value, such as managed security or power consumption.

- **Voice & messaging:** Telephony will be 150 years old in 2026. By 2030, we'll still be making some retro-style "phone calls," although it will seem even more clunky, interruptive, unnatural, and primitive than today. (It won't stop the cellular industry from spending billions upgrading to Vo6G, though.) SMS won't have disappeared, either. But most consumers will communicate through a broad variety of voice and video-interaction models, in-app, group-based, mediated by an array of assistants, and veracity-checked to avoid "fake voice" and man-in-the-middle attacks of ever-increasing subtlety.

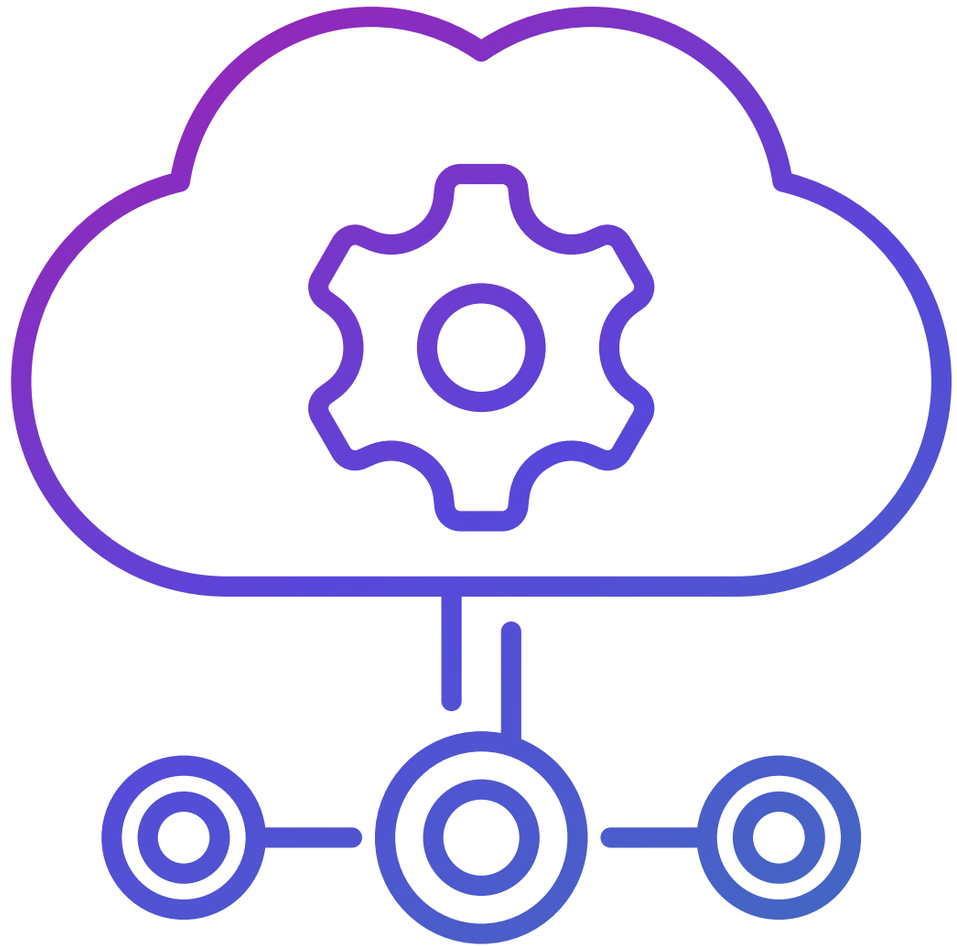
- **Enterprise comms:** Collaboration tools will progress steadily, if unspectacularly — although with ever-more cloud focus. There will be more video, more AI-enriched experiences for knowledge management, translation, whispered coaching, and search. There will be attempts to reduce travel to meetings and events as carbon taxes bite, although few will come close to the in-person experience or effectiveness. More communications will take place "contextually" — within apps, natively supported in IoT devices, or with AI-based assistants. Contact centers and customer interactions will be battlegrounds for bots and assistants on both sides. ("Alexa, renegotiate my subscription for a better price — you have permission to emulate my voice"). Security and verification will be highly prized — just because something is heard doesn't mean it will match what was originally spoken.

- **Network ownership models:** Some networks of today will still look mostly like “telcos” in 2030, but as I wrote in this post, the first industry to be transformed by 5G will be the telecom industry itself. We’ll see many new stakeholders, some of which look like SPs, some which are private network operators, and many new forms of aggregators, virtual operators, and wholesale or neutral mobile/fiber providers. I think regulations will favor more sharing of assets where it makes sense. Individual industries will take control of their own connectivity and communications, perhaps using standardized 5G or mild variations of it. There will be major telcos of today still around, but most will not be providing “slices” to companies and offering deep cross-vertical–managed services.

I could go on at length about many other topics here — autonomous and connected vehicles, the future of cities and socio-political spheres, shifts in entertainment models, the second wave of blockchain/ledgers, the role of human enhancement and biotech, new sources of energy and environmental technology, new forms of regulation, and so forth. But this list is already long enough, I think. This is a vision for 2030, which I hope is self-consistent and reasonable — but it is not the only plausible future scenario.

LoRaWAN and Wi-Fi: Made for Each Other

By Remi Lorrain, *LoRaWAN Ambassador, Semtech*



If you're in the process of implementing the internet of things, you've probably spent a lot of time researching wireless connectivity solutions, for which there are many (perhaps too many) choices. However, two—Wi-Fi and LoRaWAN — have a synergy that makes them very appealing as an end-to-end solution from the edge to the cloud. It's the reason they're being used together in applications from industrial facilities to entire cities throughout the world. To see why, let's examine how they work so well together.

The IoT requires connectivity from the edge devices, such as various types of sensors, to the internet. At the edge, a typical protocol choice is one of the 802.15.4-based standards, Bluetooth or Wi-Fi, as each

one has mesh-networking capability. From there, the data is transmitted to a gateway and, after that, to the internet via either cellular or a low-power wireless area network.

Wi-Fi is the only protocol that can deliver blistering data rates, but its access points consume lots of power. Wi-Fi also has a line-of-sight range of only about 200 meters, uses channel bandwidths of 20 MHz or more, and, as it operates at 2.4 and 5 GHz, doesn't penetrate structures as well as lower frequencies. In contrast, edge devices using LoRaWAN consume microamps of current and can operate for years on a coin-cell battery. The protocol uses very narrow channel widths of 500 kHz or less and a maximum transmit power of 20 dBm (50 mW). Additionally, operation from 914 to 928 MHz in North America enables structure penetration and inherently long range.

The last metric, long-distance coverage, might seem counterintuitive for a technology whose transmit power is minimal and antennas are often electrically short. But because the LoRa radio uses chirp-spectrum modulation and a correlation mechanism based on band spreading, even extremely weak signals 19.5 dB below the noise level can be demodulated by the receiver. Not surprisingly, hobbyists have put this to the test, and their results were impressive, even amazing. Last July, a team of tinkerers in Spain set a record — 766 kilometers (476 miles) — using balloon-mounted directional antennas and an RFM95W transceiver from Hope Electronics with RF output of 14 dBm (25 mW).

Why not just LoRaWAN alone?

It might be logical to assume that LoRaWAN could simply be used alone rather than in combination with Wi-Fi, as it provides everything necessary for an end-to-end solution and is used this way very successfully in more than 140 countries throughout the world. However, Wi-Fi can reach throughput and low-latency performance that LoRaWAN is not intended to deliver. This means that in a growing number of situations, the two very different technologies are being used together to produce solutions that neither Wi-Fi nor LoRaWAN could serve alone. This powerful combination therefore opens up an even broader array of application uses.

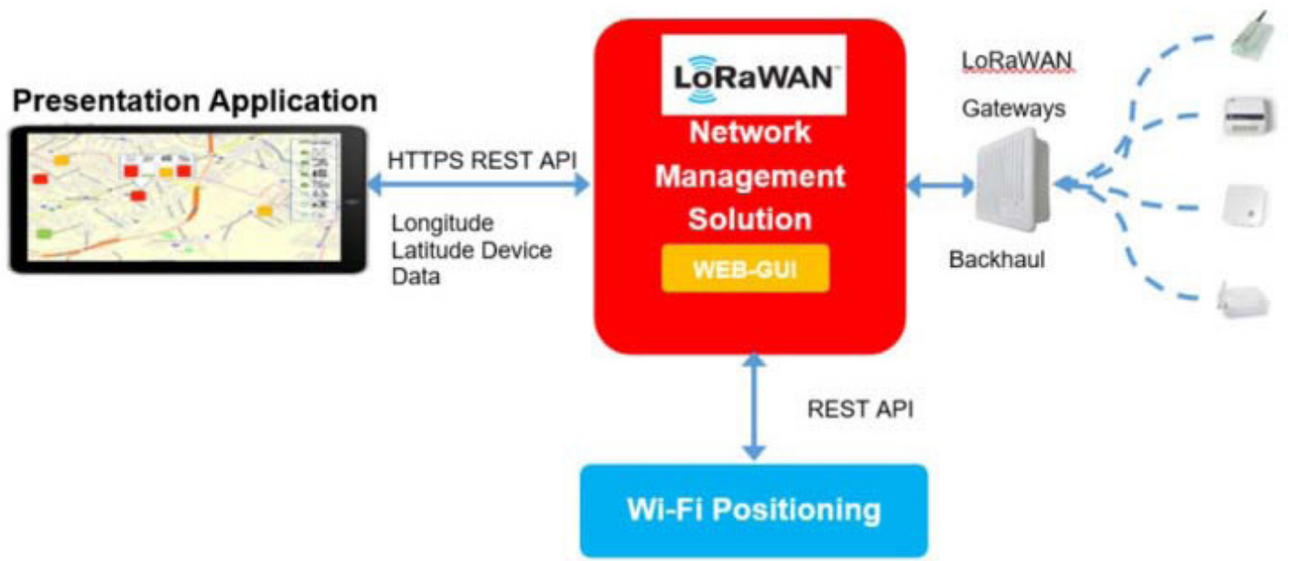
It is also remarkably easy to integrate the two. Multiple device manufacturers make transceivers and gateways that support both Wi-Fi and LoRaWAN, and Wi-Fi access point adapters are available that plug into LoRaWAN gateways. The latest LoRaWAN/Wi-Fi gateways are smaller than their predecessors, typically about the size of two smartphones stacked together, and their cost is decreasing to price points lower than even standard

consumer Wi-Fi access points. Many also include support for Bluetooth, GPS, and all of LoRaWAN's features, including multiple levels of security. Setting up a dual-protocol gateway is a simple process via the gateway's software or a smartphone app.

The process of moving data generated by LoRaWAN sensors to Wi-Fi is accomplished almost instantaneously and can be tailored to activate on specific conditions. For example, when a camera using LoRaWAN detects motion and video recording begins, transmission can be handed off to Wi-Fi, which has the bandwidth and speed required to send it to the cloud.

Another example is location and tracking, where the LoRaWAN sensor "sniffs" for Wi-Fi access points and transmits the number of satisfactory access points to the LoRaWAN cloud, after which geolocation is achieved through triangulation and precise time stamping. Even a single IoT device can achieve Wi-Fi–based geolocation accuracy of about 10 meters indoors, depending on the number of available Wi-Fi access points. Vertical elevation positioning can achieve about 5 meters, with five strong Wi-Fi signals, and outdoors in urban areas can achieve about 20 meters.

Accuracy can also be increased when fine timing measurements (also called round-trip time, or RTT) available with the IEEE 802.11mc standard are employed. IEEE 802.11mc is one of the least known recent advances in precise location technologies, as it hasn't gotten much media attention until recently. It was incorporated in Android P and is expected to become more widely deployed in the coming years. IEEE 802.11mc can increase positioning accuracy to about 1 meter and provide vertical (z-axis) location information,



LoRaWAN and Wi-Fi complement each other.

Figure 19 - Wi-Fi & LoRaWAN location services

which has eluded a solution in the past.

Wi-Fi RTT reduces location error to about 1 meter in *all three axes*, making it possible, for example, for first responders to locate someone using a smartphone to call 911 and be precisely located in an apartment in a multistory building. When RTT-enabled Wi-Fi access points and LoRaWAN are used together, this same precision extends to remote locations as well.

LoRaWAN and Wi-Fi simply play well together, something that cannot be said for other wireless communications technologies, whether short- or long-range. Cellular networks can accomplish most of what LoRaWAN can but require much more infrastructure, are more costly to deploy, consume more device battery lifetime, and give you limited control over your IoT communications network. As a result, LoRaWAN has risen to become the most widely deployed LPWAN technology, and thanks to Wi-Fi's extremely high data rates over short distances, it trumps all other solutions by an order of magnitude. Together, they offer a unique solution.

How Secure Is Your LoRaWAN IoT Device?

By Ann R. Thryft, *Contributing Editor, EE Times*

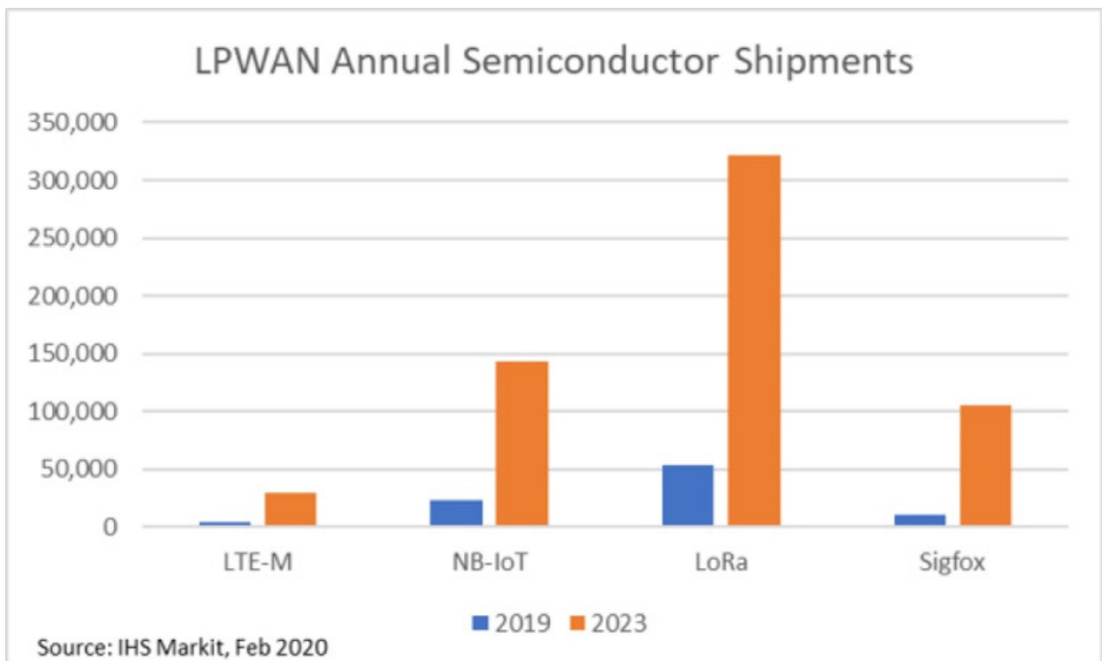
Low-power wide-area networks (LPWANs) are helping drive the internet of things explosion. They connect millions of low-power IoT and industrial IoT (IIoT) devices into wireless networks over a range of distances, from short to really, really long, from indoor applications to those covering large fields or even cities. But device designers using the LoRaWAN standard may be lulled into thinking that just configuring its security keys is enough to prevent their devices from being hacked. A new report says it isn't.

Four protocols give enterprises a choice in LPWAN connectivity: cellular NB-IoT, LTE-M, Sigfox, and the non-cellular LoRaWAN standard. Among these, the open LoRaWAN overwhelmingly dominates. Omdia (formerly IHS Markit — Technology) projects a "quite high forecast" for LoRa, said Lee Ratliff, senior principal analyst, connectivity and IoT.

According to the LoRa Alliance, LoRa is used for M2M communications in over 100 million IoT and IIoT devices in industries such as manufacturing, smart cities, smart utilities, vehicle tracking, and health care.

But with all this wireless traffic, how secure are the nodes of these networks? Not very, concludes a new white paper from IOActive Research on LoRaWAN implementation. Devices are susceptible to hacking, especially those built with revision 1.0 of the standard, including 1.0.2 and 1.0.3, |the majority of deployments so far.

LoRaWAN's mechanisms are well designed to transmit data securely, and the protocol has frequent security revisions. Its vulnerabilities lie mainly in how encryption keys are implemented and managed for network-level and application-level communications among IoT/IIoT devices, gateways, and servers. When these aren't handled correctly, LoRaWAN deployments become easy targets for hackers and other threat actors. In some deployments — such as process control, automated manufacturing, or energy utilities — results could range from inserting false sensor data to halting electrical service to interrupting communications in industrial process equipment operations, with potentially harmful effects.



Omdia LPWAN shipments 2019 vs. 2023
(Image: Omdia)

LoRaWAN security holes are avoidable

The problems arise when certain key source code is not replaced before deployment, the same keys are used for a group of devices, or keys are not strong enough to prevent reverse-engineering. If a hard-coded key is compromised, it can't be changed.

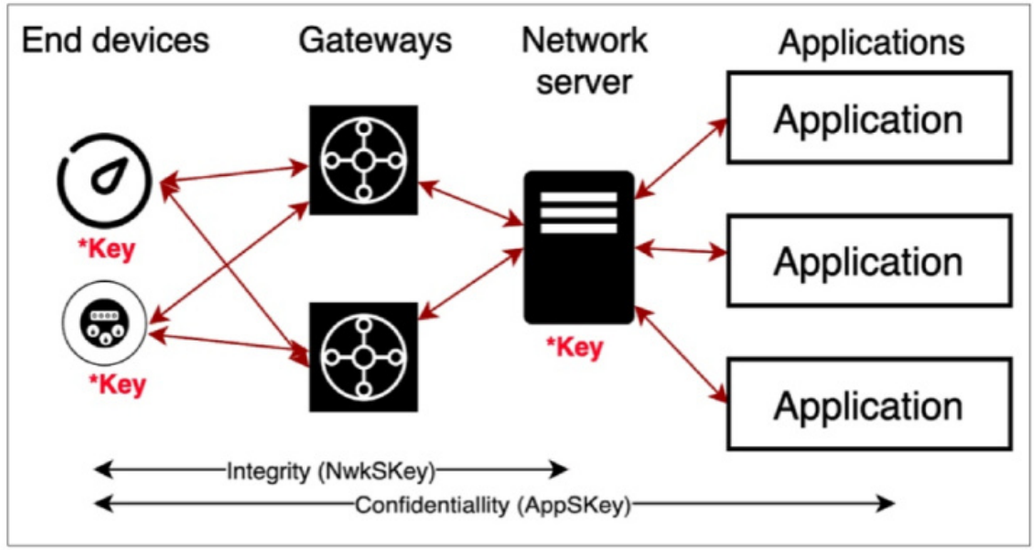
IOActive's researchers also found that tags containing certain information are not always removed before device deployment, that device firmware can be cloned if certain procedures aren't followed, and that some

internet-connected LoRaWAN servers use default or easy-to-guess credentials and can be easily hacked to access the keys.

In more common cybersecurity faux pas, some of these servers were incorrectly configured or found to be running outdated or unpatched software. Because LPWAN is open, source code can also be easily be obtained online. Other problems the report discusses are not specific to LPWANs, such as data breaches or hacking of device manufacturer or service provider networks.

"Most nodes deployed today are not 1.1, and the first version of LoRa had no provision for over-the-air [OTA] firmware updates," said Ratliff. So these nodes probably won't be updated because of their customized implementation and the problem of downtime disrupting service.

There's also no firmware over-the-air (FOTA) update mechanism in LoRaWAN 1.0. "Even if there was, the hardware has to be capable of [it] — which adds cost because more flash memory is required to hold both firmware images until the update is complete — and there's a real risk that FOTA could brick a percentage of the nodes or otherwise cause disruption," he said. "With 1.1, if you're deploying LoRa and need to do an OTA update, that would not be an issue. But the manufacturer using LoRa must enable that."



Session Keys and Functions in LoRaWAN v1.0.3

LoRaWAN provides two layers of security for communication from end device to gateway and from gateway to network server: network-level and application-level. Each uses two 128-bit encryption keys. Data integrity between network server and application server is not defined by the protocol but is left to the service provider.
(Image: IOActive)

Perhaps most alarming, these vulnerabilities aren't well-known, said Cesar Cerrudo, lead author of the white paper and IOActive's CTO. Organizations are blindly trusting LoRaWAN because it uses encryption, but that encryption can be easily bypassed if hackers can access the keys, and that's easy to do in several ways. There's also not enough awareness of cybersecurity issues

among users, who assume that just because the protocol has encryption, security keys are enough to protect communication. Some manufacturers might add encryption to their LoRaWAN devices, but it might not be good enough, as they're not cybersecurity experts.

Also, no tools exist for testing networks or detecting cyberattacks, said Cerrudo. The company has released an open-source set of tools, the LoRaWAN Auditing Framework, so that users can audit and penetration-test their infrastructure's security. The report itself contains techniques for detecting possible cyberattacks with the help of these tools, as well as best practices and basic security hygiene for LoRaWAN implementation.

Tanner Johnson, Omdia's senior analyst for cybersecurity technology, confirmed the lack of cybersecurity tools. "While there may be some private, custom implementations of security tools for monitoring, detecting, and preventing cyberthreats on LPWANs, there aren't any such tools widely available that are customized for individual protocols," he said. "In IoT cybersecurity, the primary objective is visibility."

Problem probably not limited to LoRaWAN

Cerrudo said that IOActive chose LoRaWAN to investigate because of its popularity and open technology, unlike the proprietary Sigfox, although Sigfox has security issues, too, including similar problems with handling keys. With LTE-M and NB-IoT, users generally rely on the wireless communications service provider for security.

Other LPWAN standards have probably not been examined as closely as the popular LoRaWAN, so it isn't known yet if they're easier or more difficult to implement securely, said Ratliff. "LTE-M borrows from the LTE standard that's been scrutinized quite a bit. So a lot of people think it's just as safe as LTE. NB-IoT is new and getting as much attention as LoRa. But it's not as commonly deployed outside of China, so it may not be in the same boat." Most likely, vulnerabilities will eventually be discovered for NB-IoT, too.

It's important to remember the security differences between wired versus wireless, said Ratliff. Wireless networks are more vulnerable than wired because in them, the attack surface is every node, not just a single gateway requiring physical access. With wireless protocols, hackers can access nodes remotely, so there's little risk. That means that even with a secure network, they're always trying.

Unlocking 6 GHz Is More Necessary Than Ever

By Ian Adams, *Associate Fellow, TechFreedom*

After over a month of necessary isolation, Americans have a better appreciation than ever for the role of technology in their lives. It's no exaggeration to state that Wi-Fi–enabled devices have kept portions of the economy moving, children in classes, doctors in touch with patients, and families connected. And as important as Wi-Fi is today, its significance is poised to grow even more in the months and years to come. Given that trend, it is surprising to observe a movement afoot that would hamstring Wi-Fi's future.

Wireless spectrum is a finite resource. As more and more Americans avail themselves of high-speed internet, an outcome that all policymakers would do well to seek, the need for spectrum that can support their demands

grows. The 6-GHz band is valuable for exactly this reason. It represents a broad swath of spectrum capable of sustaining not only novel and higher-speed internet applications but also bringing more Americans online in urban and rural areas alike.

Utility providers, like the gas and petroleum industries that currently utilize the spectrum, contend that Wi-Fi devices operating on the 6-GHz band will result in radio interference that will degrade the reliability of their network and impinge upon their ability to operate. Yet continued reliable utilization of the 6-GHz band by utilities and Wi-Fi's access to the band are not mutually exclusive; the FCC's approach — the culmination of years of study — carefully and thoughtfully ensures that. The FCC has a proven track record for balancing the needs of licensed and unlicensed operators in the same band of spectrum.

As proposed, the FCC's vision for unlicensed use of the 6-GHz band is predicated on the bedrock principle that the operation of utilities within the band is vitally important. In fact, under the FCC's proposal, utility access is primary. Wi-Fi devices operating in the 6-GHz band, for their part, would be divided into three classes, each with its own technical limitations designed specifically to prevent interference. For instance, low-power devices like home routers would be limited to about one-quarter the power of today's devices and would be prohibited from being portable or battery-operated (to prevent the possibility of their use outdoors).

In spite of demonstrated sensitivity to the ability of incumbents to utilize the 6-GHz band, utilities are persisting in their claims that the FCC's action would harmfully interfere with their operations. As a simple matter of administrative expertise, there are claims that the FCC is proceeding blind to the possibility of interference beggar belief. Unreliable access to the 6-GHz band would work to the detriment of both the utilities and the millions of Americans reliant upon Wi-Fi routed through the band.

As the nation's primary expert agency charged with ensuring reliable access to wireless spectrum, the FCC is the body best positioned to weigh technical claims about radio interference. In that capacity, the FCC has overseen a lengthy and exhaustive process to determine whether unlicensed sharing in the 6-GHz band is possible — and they have concluded that it is. Their judgement is not beyond question, but after years of gathering information and engineering analyses on the subject, it is the best-informed government voice on the matter.

On the basis of its finding that Wi-Fi will not cause harmful interference in the 6-GHz band, it is now vital that the FCC move forward quickly to ensure that Americans have access to the capabilities that Wi-Fi in the 6-GHz band will enable within the next year. Unlocking the 6-GHz band today is both timely and necessary.

Addressing the Multiple Layers of Constraints of Wireless Network Design

By Jocelyn "Justin" Lauzon, *Senior Communications Engineer, Reflex Photonics*

Wireless network design is complex. Communications engineers are involved at the core of the effort, of course, but other constraints associated with the deployment of the antenna network need to be considered from the get-go in order for the network to have a chance to become a reality and a long-term success. Lawyers, urbanists, meteorologists, and even possibly local anthropologists need to be involved in one form or another, in combination with the engineers. Other communication network design efforts also need to consider multidisciplinary activities in their process,

but none so much as wireless networks.

If the wireless design is based on using existing antenna infrastructures on which communication cells can be added at reasonable cost from a neutral supplier, then these additional constraints are greatly attenuated. We will focus on the worst-case scenario in building a wireless network. What constraints need to be addressed?

Formula for needed communications capacity

Of course, it starts with the service offering, the "real" communications engineer work. The capacity to be offered must be evaluated for each area to be covered by the network. Knowing how the need for wireless bandwidth is increasing with time, a provision must also be considered for future needs to avoid having to upgrade the network too often. Each wireless service provider has its own formula to calculate the needed capacity. The formula considers the type of customers to be served in the area: residential, industrial, or "transport captive." By "transport captive," we mean large streets or highways covered by the network. The residential area is less demanding in terms of capacity but much more so in terms of social acceptability of the presence of antennas in the neighborhood (we will get back to this later). The market shares that the supplier is targeting also come into play in the calculation of the needed capacity per area. The network can certainly be inhomogeneous in terms of capacity versus area if the area itself has an inhomogeneous urban plan. Once the total and distributed needed capacity is calculated, the next step is to figure out the connection to a wired network and the access to the needed bandwidth from this larger network that will ensure connection to the rest of the world.

Coverage

Dead zones must be avoided, considering the worst possible environmental conditions for signal transmission. By environmental conditions, we mean the weather, but we also mean potential electromagnetic interference in the area; information that needs to be measured on the field and then analyzed before undertaking the design. You want to obtain the necessary coverage for the best return on investment regarding antenna deployment. Thus, you want to limit the total number of antennas to be installed. Your network architecture should also offer redundancy, knowing that the quality and continuity of service is one of the keys to get the targeted market shares. Should the architecture be mesh, start, ring, a mix of all, or even something else having to consider the constraints associated with antenna deployment? Adding power to the signals to ensure coverage is not always the solution, as regulations limit this amount of power, even more so in residential areas, and these regulations also limit the antenna

configurations (height in particular) that could help get the needed coverage.

Legal, urbanistic, and weather constraints

Lawyers are needed to ensure land rights and rights of way for the antennas to be deployed, as well as for the potential disputes when the network plan needs to be approved by local authorities.

Urbanists are needed to try to avoid these disputes by considering antennas that will blend in with the decor as much as possible. These urbanists can also help with the consideration of how the local population could respect or not respect the antenna footprint and surroundings to avoid accidents/damage and allow easy and secure access for future regular maintenance and repair. These antennas need to be accessed without being accessible.

Meteorologists must be consulted to evaluate the worst potential weather condition for signal transmission in that geographical zone, as well as for temporary or permanent damage to the antennas that could be caused by extreme storms, depending on their configuration.

Social acceptance and regulations

Local anthropologists, or at least a local representative knowing the fabric of the people living in that area, should also be consulted upfront to avoid potential disputes and try to ensure social acceptability of the project. Everyone wants and needs a good wireless network coverage, but it seems that nobody wants to have to even so much as see the tip of an antenna from their backyard. Compromise is key, but with social networks, greatly supported by wireless communications, compromise is more difficult when an annoyance becomes a cause for someone that feels empowered by that cause.

The service supplier should also have constructive discussions with local authorities all through the design process to ensure considering the regulations and unwritten constraints upstream rather than face a rebuttal when the final project is submitted for approval.

Making it work

How do all those people work together efficiently to ensure a successful wireless network design leading to a deployment that will satisfy the users and the local citizens? That is an excellent question. The communications engineers should remain the key actors in the process, but other than that, the blend of contributors must be managed with patience, openness, and persistence.

In the circumstances, minimizing the number of antennas in the network to minimize total cost should not be the main priority; only one of the factors should be considered to get to the best possible acceptable project.

Conclusion

Avoiding one of these multidisciplinary aspects during the wireless network design process will probably save time regarding the draft of the first revision of the final project, but it could backfire into having to redo the whole design from nearly the ground up if the rebuttal from the local authorities and population is strong. It will also make Revision 2 of the project so much more difficult to be approved. Thus, the key to the design of a wireless communications network is simply communications, preferably face-to-face in some occasions.

Resources

Webinar — Wireless IIoT: Making Factories Smart and Flexible

Rohde & Schwarz Video Series — MWC2020

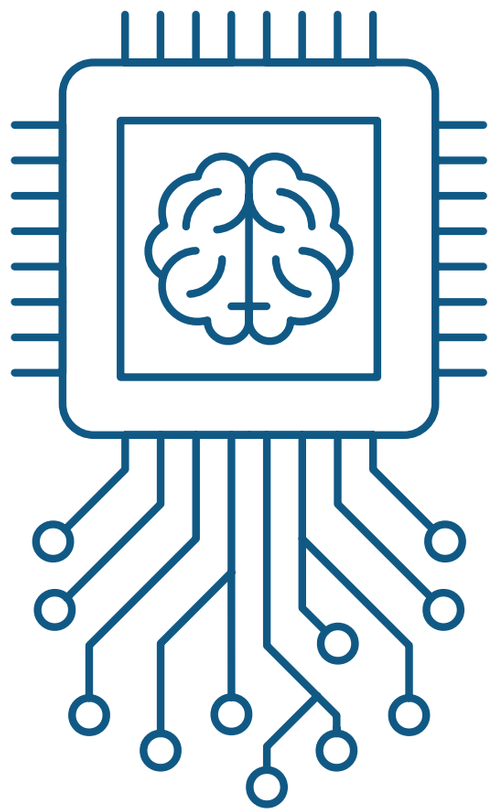
Rohde & Schwarz Video Series — Let's Talk IoT

Webinar — Everything You Need to Know About Bluetooth® Low Energy

Get Your NB-IoT Poster and Have the Overview

Next-Gen UWB Uses Digital RF and ML to Improve Accuracy and Power

By Nitin Dahad, *Staff Correspondent, AspenCore*



Imec announced in May that it has developed next-generation ultra-wideband (UWB) technology that uses digital RF and machine learning (ML) to achieve a ranging accuracy of less than 10 cm in challenging environments while consuming 10× less power than today's implementations.

The research and innovation hub announced two new innovations from its secure proximity research program for secure and very high-accuracy ranging technology. One is hardware-based, with a digital-style RF circuit design such as its all-digital phase-locked loop (PLL), to achieve a low power consumption of less than 4 mW/20 mW (Tx/Rx), which it claims is up to 10× better than today's implementations. The second is software-based enhancements, which utilize ML-based error-correction algorithms to allow less than 10-cm ranging accuracy in challenging environments.

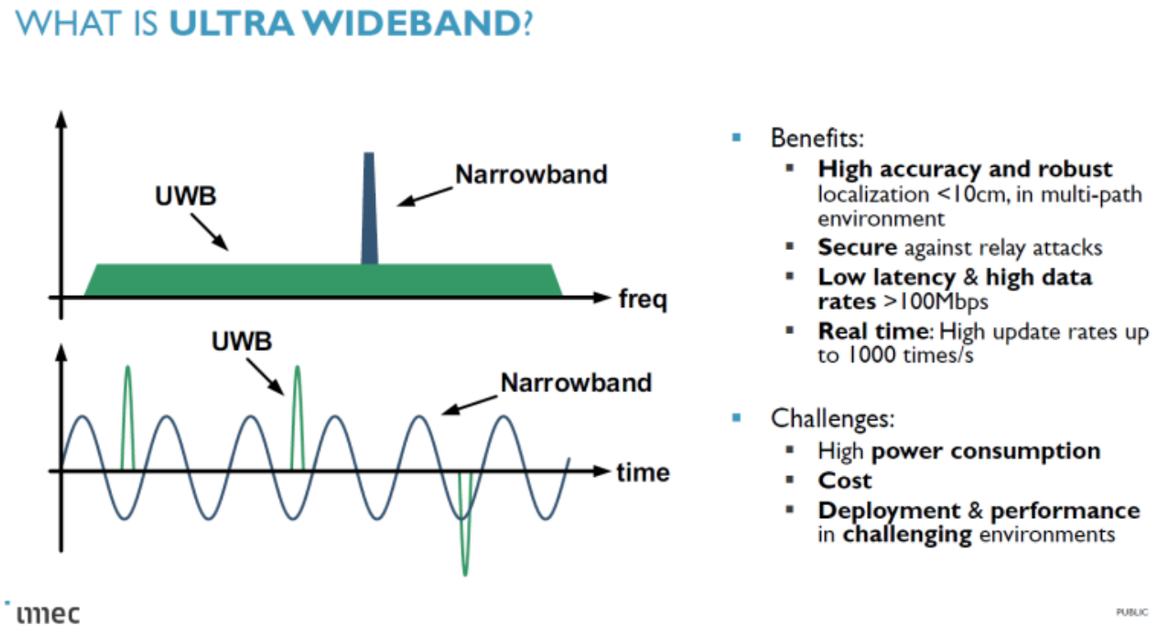
Explaining the context, imec said that

UWB technology is currently well suited to support a variety of high-accuracy and secure wireless ranging use cases, such as the “smart lock” solutions commonly being applied in automotive; it automatically unlocks a car’s doors as its owner approaches and locks the car when the owner moves away.

However, despite its benefits, such as being inherently more difficult to compromise than some alternatives, its potential has largely remained untapped because of its higher power consumption and larger footprint. Hence, imec said that the hardware and software innovations it has introduced mark an important step to unlocking the technology’s full potential and opens up the opportunity for micro-localization services beyond the secure keyless access for which it’s been widely promoted to AR/VR gaming, asset tracking, and robotics.

Christian Bachmann, the program manager at imec, said, “UWB’s power consumption, chip size, and associated cost have been prohibitive factors to the technology’s adoption, especially when it comes to the deployment of wireless ranging applications. Imec’s brand-new UWB chip developments result in a significant reduction of the technology’s footprint based on digital-style RF concepts: We have been able to integrate an entire transceiver — including three receivers for angle-of-arrival measurements — on an area of less than 1 mm².”

He added that this is when implemented on advanced semiconductor process nodes applicable to IoT sensor node devices. The new chip is also compliant with the new IEEE 802.15.4z standard supported by



UWB benefits and challenges (Image: imec)

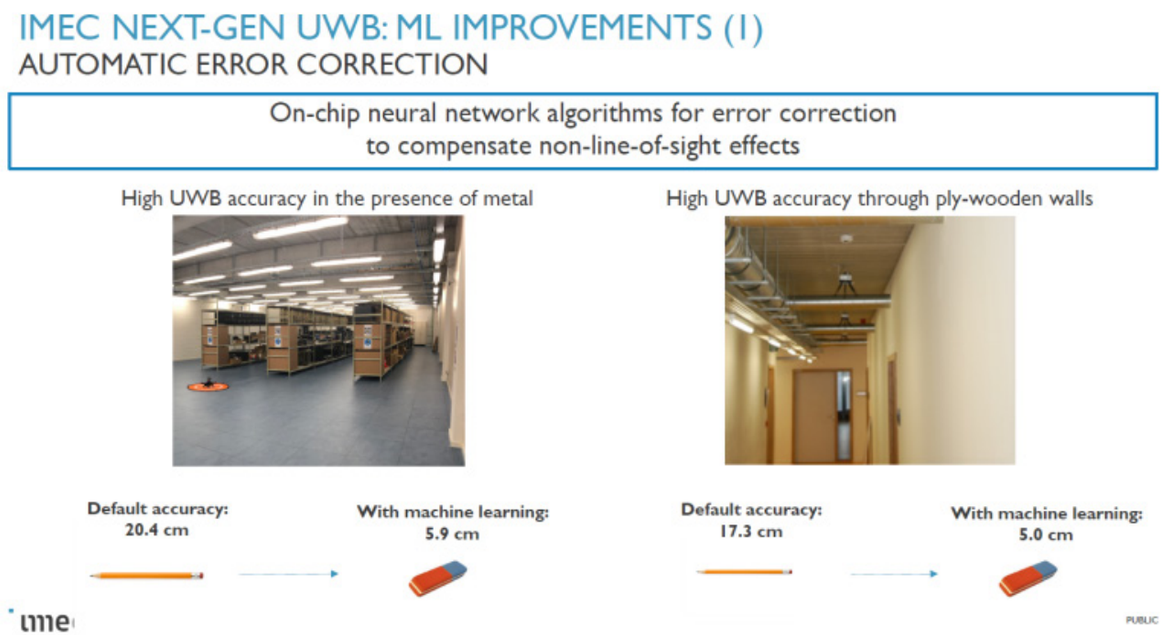
high-impact industry consortia such as the Car Connectivity Consortium (CCC) and the FiRa (“fine ranging”) Consortium.

Complementing the hardware developments, researchers from IDLab (an imec research group at Ghent University) have come up with software-based enhancements that significantly improve UWB’s wireless ranging performance in challenging environments. This is particularly in factories or warehouses where people and machines constantly move around and with metallic obstacles causing massive reflection — all of which impact the quality of UWB’s localization and distance measurements.

Using machine learning, it has created smart anchor selection algorithms that detect the (non) line of sight between UWB anchors and the mobile devices that are being tracked. Building on that knowledge, the ranging quality is estimated and ranging errors are corrected. The approach also comes with ML features that enable adaptive tuning of the network’s physical layer parameters, which allows appropriate steps to then be initiated to mitigate those ranging errors — for instance, by tuning the anchors’ radios.

Professor Eli De Poorter from IDLab said, “We have already demonstrated a UWB ranging accuracy of better than 10 cm in such very challenging industrial environments, which is a factor-of-2 improvement compared to existing approaches. Additionally, while UWB localization use cases are typically custom-built and often depend on manual configuration, our smart anchor selection software works in any scenario, as it runs in the application layer.”

Through these adaptive configurations, the next-generation low-power and high-



Obstacles and non-line-of-sight effects can impact the quality of UWB’s localization and distance meaurements. On-chip ML can correct errors, as shown in these two examples.
(Image: imec)

accuracy UWB chips can be utilized in a wide range of other applications, such as improved contact tracing during epidemics using small and privacy-aware devices.

In fact, imec has already licensed the technology to its spinoff, Lopos, which has released a wearable that enables enforcement of Covid-19 social distancing by warning employees through an audible or haptic alarm when they are violating safe-distance guidelines while approaching each other.

Choosing UWB instead of Bluetooth, Lopos's SafeDistance wearable operates as a standalone solution, which weighs 75 g and has a battery life of two to five days. The UWB-technology–based device enables safe, highly accurate (<15-cm error margin) distance measurement. When two wearables approach each other, the exact distance between the devices (which is adjustable) is measured and an alarm is activated when a minimum safety distance is not respected.

Because it is standalone, no personal data is logged and there is no gateway, server, or other infrastructure required. Lopos has already ramped up production to meet market demand, with multiple large-scale orders received over the last few weeks from companies active in a wide range of different sectors.

Touchless and Short-Range Wireless: A Path to Normality Beyond Covid-19?

By Nitin Dahad, *Staff Correspondent, AspenCore*

As many countries gradually come out of lockdown, there is still going to be fear among many for a long time about going back to life as it was. Maybe it won't be the same as it was, but one thing is certain: Many people will want to feel assured when they go about their daily routines that they don't face avoidable risks of picking up the virus and being part of the second wave.

To address this, many technologies are now being fast-tracked to deployment, some of which may not have seen such rapid market traction prior to Covid-19. But we're in a new world, where anything goes. I've listened to many debates about the widespread penetration of technology, data capture, and video platforms' intrusion into our lives progressing unregulated, with the subsequent dangers that possibly lie ahead in terms of privacy and security.

Two technologies that could play a

key role in providing public assurances in daily life are touchless technologies and short-range wireless technologies, such as Bluetooth Low Energy (BLE) and ultra-wideband (UWB).

Taking wireless technologies first, in an interview this week with Wenjun Sheng, co-founder and CEO of Telink Semiconductor, he cited examples of wearable devices with BLE chips enabling social-distancing awareness and even enforcing quarantine. One such example is in Hong Kong's BLE wristbands issued to incoming passengers to monitor and ensure adherence to the 14-day quarantine requirements. Another recent BLE-based wearable is the Bump device, which alerts people when they are too close. It is primarily designed to ensure workplace safety, much like the UWB-based SafeDistance wearable introduced by imec spinoff Lopos.

The argument for UWB rather than BLE is the greater accuracy that can be achieved

The BLE wristbands, which passengers arriving in Hong Kong must wear for the 14-day quarantine period
(Image: Office of the Government Chief Information Officer)

with UWB. But Telink's Sheng said that, in real-life situations, UWB can still creep up to tens of centimeters' accuracy, while BLE incorporates features that can improve the accuracy to about 1 meter. It then depends on the tradeoff that can be achieved between accuracy and power consumption. With its BLE business growing by 50% every year, Sheng told us that Telink is working on using algorithms in its devices that could increase the accuracy of its devices to match the accuracy of UWB devices.

The touchless path to seamless user experiences

Another area that could provide a path to providing consumers further assurance to return to some kind of normal is touchless technologies. According to research carried out by Ultraleap, a haptics technology developer, the public is concerned about the risk of picking up bacteria from touchscreens. The company added that the average supermarket checkout touchscreen is used as often as 350 times a day by different consumers, which means the screen can easily be contaminated.

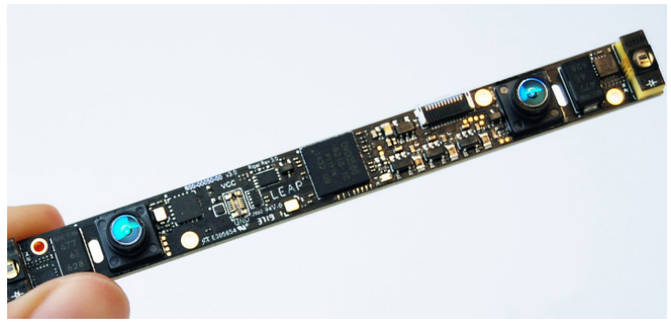
Setting the background, Ultraleap said that a study published in the American Journal of Infection Control indicated that

Touchscreens invariably have bacterial colonies on them, and a study indicates that touchless interfaces would give the public assurances that they would be more hygienic.
(Image: Ultraleap)

100% of the 17 public grocery store touchscreens tested were found to have bacterial colonies on them, and 59% were found to have dangerous bacteria, such as E. coli. All 17 touchscreens also had bacterial colonies. In the U.K., a 2009 study of London's public transport network and a public space in a hospital showed that more than 60% of touch surfaces had high levels of bacterial contamination.

In its research among 538 consumers in the U.K. and U.S., Ultraleap said that only 12% believed that touchscreens in public spaces are hygienic, while more than 82% on average (79% in the U.S. and 85% in the U.K.) were confident that touchless interfaces would be more hygienic and give them better protection.

In its white paper with the results of the study published this week, Ultraleap said that the three main alternatives to touchscreens are gesture control, which tracks the position of a user's hands; voice control, using voice-recognition software; and mobile apps used to connect to public screens. The firm obviously points to the data suggesting that touchless gesture-based interfaces are expected to be preferred as a future option over touchscreens, counter service, or mobile apps. It believes that gesture-control technologies will play a significant role in restoring consumer confidence in retail and other public environments in a post-Covid-19 world.



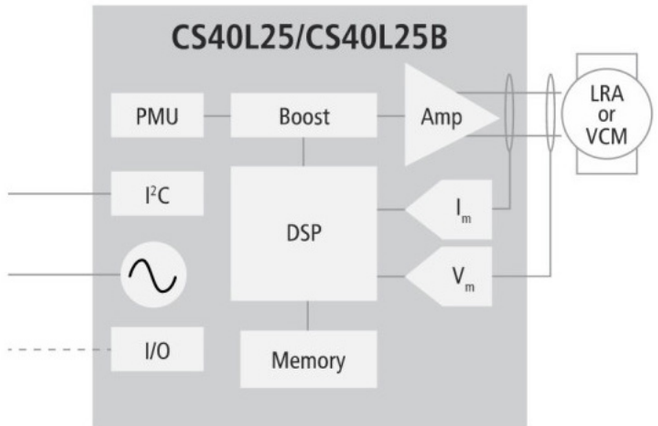
Ultraleap's Rigel module captures the movement of a user's hands and fingers and can be retrofitted to existing concepts and hardware to enable touchless interfaces.
(Image: Ultraleap)

Its hand-tracking module, the Ultraleap Rigel, can be retrofitted to existing concepts or hardware and is designed for integration into both consumer and enterprise-grade products. It captures the movement of a user's hands and fingers, being able to discern 27 distinct hand elements in a 160° × 160° field of view and tracking up to 75 cm. With a 90-Hz refresh rate on USB2 and low-latency software, the time between motion and photon falls beneath the human-

perception threshold.

Mechanical buttons are also an area where the need to touch can be eliminated. Cirrus Logic announced in May its CS40L25 family of boosted haptic drivers to enable OEMs to create customized user experiences beyond the single-action response of mechanical buttons. These can help create context-aware virtual buttons for almost any surface. The company said many smartphone designers are leading this behind-the-screen design evolution to increase haptic feedback solutions by replacing peripheral button functions. Automobiles, PCs, wearables, and game controllers are also moving beyond traditional button interfaces to incorporate non-mechanical haptic feedback.

Its CS40L25 products integrate a high-performance haptic driver, a digital signal processor, and a boost converter. The devices



Cirrus Logic's CS40L25 products integrate a high-performance haptic driver, a digital signal processor, and a boost converter.
(Image: Cirrus Logic)

are resonance-aware, drive high-performance linear resonant actuators (LRAs) and voice coil motors (VCMs), and enhance user experiences by supporting unique/pre-stored haptic waveforms. Ultra-low latency provides real-time control of the haptic motor. This provides users with a more immediate sensation or response. Closed-loop algorithms maximize LRA effectiveness and enable strong and consistent haptics with a crisper, less "buzzy" effect.

Cirrus Logic said that it recently started sampling its next-generation haptic product, which integrates force sensing and a haptic driver. The single-chip device is anticipated to improve performance, reduce power consumption, and simplify system design with up to a 50% reduction in the overall footprint of a smartphone haptic subsystem. The haptics technology market is expected to grow by $13.58 billion during 2020–2024, according to market research firm Technavio, indicating a 16% CAGR growth. It said that key players include AAC Technologies, Alps Alpine, Analog Devices, Cypress Semiconductor, Dongwoon Anatech, Imagis, Immersion, and Microchip.