AI-based RF Awareness for Private Wireless Networks

iGR

AI-based RF Awareness for Private Wireless Networks

A White Paper

Published Third Quarter, 2022
Version 1.0

iGR
12400 W. Hwy 71
Suite 350 PMB 341
Austin TX 78738

Table of Contents

Executive Summary

Enterprise and government facilities considering private LTE/5G networks are generally in the learning and discovery phase of what they need and the best approach to meet their needs. As new private wireless networks are deployed, the need to maintain network performance, lower TCO, implement and manage security, and protect corporate assets will require new practices and tools.

RF detection addresses both the need to improve network performance and increase network security – this means monitoring and analyzing the RF environment in which the private network operates, looking for sources of interference and/or spurious RF sources or monitoring. RF detection has traditionally been carried out manually, with the operator using RF monitoring equipment to look for rogue or unauthorized RF signals – this process tends to be reactive, expensive and subject to delays or error from a myriad of externalities.

Next-generation solutions, such as OmniSIG® from DeepSig, use AI machine learning and automated, real time RF monitoring to detect real-world RF conditions and detect interfering or unauthorized RF sources many times faster, more accurately, and at lower cost than traditional approaches.

OmniSIG rapidly detects known and unknown wireless signals and anomalies in real time, allowing centralized or remote staff to simultaneously relate the wireless environment to service conditions. OmniSIG's operational improvements and greater accuracies have much lower costs than traditional methods. The benefits of OmniSIG include:

- ML-driven spectrum awareness and sensing using trained models to classify RF signals in real time
- For enterprises, OmniSIG can differentiate and identify signals within the whole environment, both within the building and across the campus
- Scans wide bandwidths quickly and efficiently and can differentiate signals using the same waveforms
- Operates with a wide range of generally available radio devices and industry leading test and measurement tool sets.

Private wireless networks are relatively new but the technologies are well understood and many enterprises, vendors, municipalities and organizations have deployed proof-of-concept and trial networks, with many more to come in the next few years. iGR forecasts that the network spending (network equipment, installation and integration) opportunity in the U.S. alone just for CBRS will reach $5.1 billion in 2026. Globally, iGR estimates the private wireless network opportunity to be in excess of $9 billion in 2026. These estimates are only to deploy the private wireless networks and do not include the opportunity for developing and deploying new applications and services.

Private wireless networks

iGR defines a “private wireless/cellular network” as one that is wholly operated by an enterprise, municipality or government entity for the benefit of that organization. The goal of the private network, therefore, is not to support paying subscribers but rather to support applications and services needed by that organization.

For example, a manufacturer may deploy a private network for communications within the facility including to machine tools, robots, automated guides vehicles and for building environmentals, security and lighting. A hospital may use a private network to connect staff in the building with each other and various applications but may also provide improved coverage to patients and guests.

Why use a private wireless network?

Private wireless networks are generally deployed for two reasons: extend/expand coverage and/or improve capacity in the building. The underlying reason for the private network deployment dictates the type of spectrum used, and each spectrum has its distinct advantages – more on this later.

The success of each private network is dependent, either in whole or in part, on the performance of the network and on network security. Similarly, network security is crucial for most private wireless deployments.

One solution that can address both the need to improve network performance and increase network security is RF detection. Simply, RF detection means monitoring and analyzing the RF environment in which the private network operates, looking for sources of interference and/or spurious RF sources.

RF optimization and maintenance has traditionally been carried out manually by the network operator using RF monitoring equipment to look for rogue or unauthorized RF signals – this process tends to be reactive, expensive and subject to delays or error from a myriad of externalities.

The latest solutions, however, such as OmniSIG from DeepSig, use machine learning, AI and real time RF sampling to detect interfering or unauthorized RF sources faster, more accurately, and at lower cost than traditional approaches.

Private wireless applications

A private wireless network is based on 4G LTE or 5G network technology and so the range of applications and use cases that can be supported is wide, ranging from the simplest of IOT applications to augmented and virtual reality apps that require high bandwidth and low latency. In general, private wireless network applications are divided into several groups, as shown in the following table.

Table 1: Private wireless network applications

Application	
Critical communications	▪ Covers all aspects of communications between users and devices in an industrial, defense or commercial environment ▪ Includes routine communications but also extends to emergency services and first responders
Neutral host	▪ Private network can support multiple external mobile operators ▪ Maintains the privacy and security of the various carriers/enterprises connected to the network
IOT (Internet of Things)	▪ Covers a wide range of applications and devices ▪ Includes building lighting and HVAC control, monitoring of utility pipelines, power plants and oil and gas pipelines, and point-of-sale solutions in retail
Fixed wireless Internet service	▪ Supported by private wireless networks ▪ Support school districts with remote classroom and learning, communities that need to close the digital divide and home broadband service to remote homes or communities
Security	▪ Includes the ability to place video cameras wherever needed in or around a building or campus and monitoring and controlling building or campus access
Augmented and virtual reality	▪ Applications in many industries ▪ Expected to play an increasingly important role in future via special AR/VR goggles/glasses and/or tablet PCs, etc for diagnosing technical problems, guiding surgery or repairs, training and instruction of complex tasks, and advertising and 'smart shopping'
Automation and control	▪ Applies to several vertical industries, especially manufacturing, healthcare, and warehouse and storage ▪ Goal is to improve the efficiency, energy consumption and safety of the facilities

Source: iGR, 2022

Applications for automated RF awareness

As discussed earlier, the success of each of these private network applications is dependent on the performance and security of the network, ease of use and cost of ownership. If network performance or reliability is compromised due to traditional or malicious interference then the operations of manufacturing lines, logistic centers, hospitals, data centers, critical communications or other private 5G users may be negatively impacted.

And, of course, network security is crucial for most of these applications. Hospitals, for example, are bound by patient confidentiality and HIPPA rules, while financial and retail organizations must protect customer financial and payment data. Manufacturing and industrial enterprises must also protect their intellectual property as well as maintain highly reliable operations.

Enterprises are also concerned about unauthorized network access and hacking. As well as resulting in ransomware attacks, poor network security can be disastrous for an oil refinery or chemical plant, nuclear power station, or gas or oil pipeline. Private networks supporting critical infrastructure must be protected and hardened as much as the infrastructure they are supporting. Continuously monitoring against threats, denial of service or jamming attempts, or degradation or manipulation of the network is key for delivering this critical layer of wireless network security which allows such facilities to adopt and rely on private 5G networks.

One of the traditional solutions to network monitoring to improve network performance (reducing TCO) and increasing network security is RF detection - monitoring and analyzing the RF environment in which the private network operates, looking for sources of interference and/or spurious RF sources or monitoring.

RF monitoring and analysis tasks are most commonly conducted by highly trained technical staff with complex RF test and measurement equipment to survey and diagnose problematic RF conditions or degraded service areas.

The traditional RF trouble-shooting cycle typically begins when a pattern of degraded KPIs (key performance indicators) and/or user complaints are received. Skilled field staff are dispatched for manual RF trouble-shooting in days or weeks after service affecting issues are noted. Field techs carry their T&M tool sets to the area of concern and begin scanning the assigned area by driving or walking around while operating their gear. After collecting field-measurements, the data is post-processed for the technical staff to begin interpreting the data and take corrective actions. After corrections are made, field measurements are typically repeated to verify the issues have been mitigated. Ongoing monitoring follows a similar procedure at prescribed intervals.

Traditional RF trouble-shooting operations can therefore be described as: reactive, expensive and subject to delays or error from a myriad of externalities. We are not saying that T&M products and RF engineering practices are entirely flawed - they have proven utility and quality and serve many functions extremely well. Rather it can be said that today's human-dependent practices have limited capacity and are costly which often delays taking corrective steps. The traditional public operator methods are neither economically nor operationally feasible for private and enterprise wireless networks.

Enterprise optimized, next-generation solutions, such as OmniSIG from DeepSig, use AI machine learning and automated, real time RF monitoring to detect real-world RF conditions and detect interfering or unauthorized RF sources many times faster, more accurately, without teams of engineering staff and at lower cost than traditional approaches.

The benefits of OmniSIG®

DeepSig launched OmniSIG® in 2017, the industry's first AI-based RF classification software product, incorporating precisely architected deep learning models for wireless signal features. OmniSIG software accurately processes massive amounts of raw RF data through trained neural networks and outputs refined structured data in milliseconds. OmniSIG is able to classify all types of signals much faster than conventional methods while running on COTS general computing hardware.

Today, OmniSIG is widely deployed in operationally sensitive enterprise facilities, next-generation defense systems and as a critical component for network resiliency and wireless threat protection. In deployments, OmniSIG is a highly agile software product which works with a wide range of radio receiver devices to collect real time RF samples from the local environment. This includes low cost to high performance commercially available software defined radios, embedded platforms and 3GPP Radio Units in the future. The radio device provides snapshots of live radio signal data as the main input to OmniSIG's neural network software deployed on-premise or centralized cloud platforms (including Azure and AWS), depending on the preferred deployment model. OmniSIG can also be deployed as an xApp in a 5G RIC (RAN Intelligent Controller) architecture.

OmniSIG detects known and unknown wireless signals and anomalies in real time, enabling centralized or remote staff to simultaneously relate the wireless environment to service conditions. Furthermore, structured data are automatically analyzed into trends and patterns which reveal greater degrees of RF situational awareness and automated detection of changes or abnormal behaviors of radio activity to be flagged proactively. OmniSIG's operational improvements and greater accuracies also have much lower costs than traditional methods.

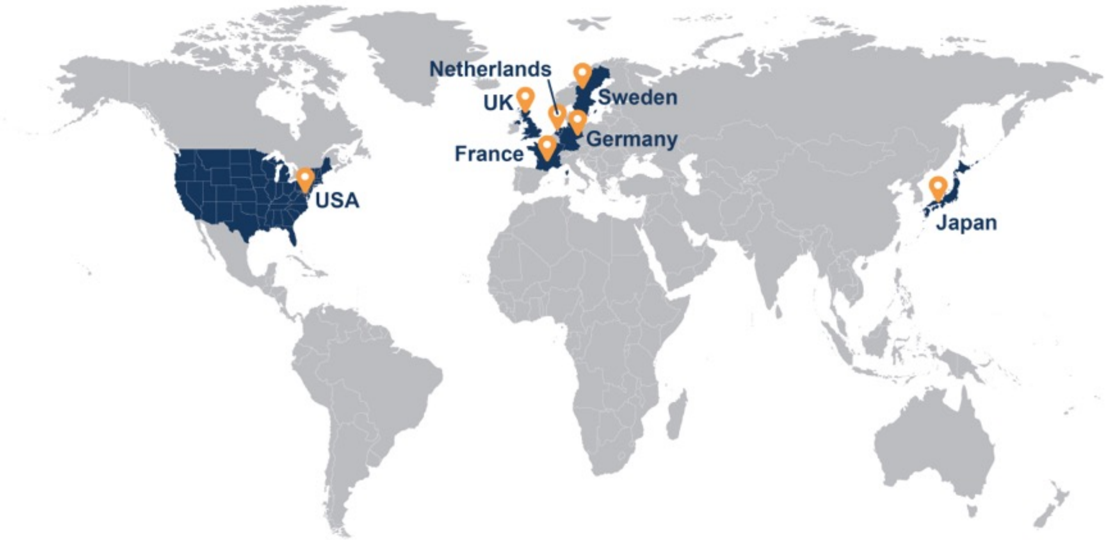
The benefits of OmniSIG can therefore be summarized as:

- ML-driven spectrum awareness and sensing
- User trained models to classify RF signals – new signal types can be quickly trained and implemented
- Can rapidly differentiate signals using the same modulations – for example, OmniSIG can differentiate between 5G, LTE and Wi-Fi, even though they use the same underlying OFDM waveform
- For enterprises, OmniSIG can differentiate and identify signals within the whole environment, both within the building and across the campus
- Scans wide bandwidths quickly and efficiently, not just specific frequencies (detects and classifies faster than traditional methods)
- Inputs raw RF data from multiple radio devices, not just one or two points in the enterprise or organization
- On-premise or cloud-based processing – provides additional security if needed

Growth of Private Wireless Networks

Private network spectrum

Shared / unlicensed spectrum is attractive because private network deployments do not require the licensed spectrum of mobile operators. Licensed sub 6 GHz spectrum bands are also used by mobile network operators to address enterprise customers. New bands of shared and unlicensed spectrum will be made available for private networks in the coming years which will increasingly require awareness and intelligent response to RF activity from in-network emissions and incumbent users.



Sub 6 GHz licensed

Various sub 6 GHz spectrum bands are used by the mobile operators around the world – many of these operators make spectrum available for private networks. Generally, the bands in use fall into three segments:

- 600 MHz - 900 MHz has been in use by many countries since cellular networks were introduced in the 1980s. These bands now support both 4G LTE and 5G networks.

- 1.7 - 2.5 GHz spectrum was introduced in the late 1990s for 'PCS' services. Again, these bands are now used for both 4G LTE and 5G networks in different parts of the world.

- Mid-band spectrum is a relatively new development – these bands are between 3.5 GHz and 4 GHz and have been licensed in most countries for 5G services.

mmWave

Another spectrum available for private networks, mmWave spectrum, is referred to as ‘millimeter’ because that is approximately the size of the wavelength. The mmWave bands of 24, 28, 37, 39 and 47 GHz are available for 5G in the U.S.; the 24 and 28 GHz bands were auctioned in 2019, and then the 37, 39 and 47 GHz bands were auctioned in March 2020. Since mmWave spectrum is licensed by the MNOs, access to these bands for a private network must be provided by the operator.

mmWave bands provide a very high throughput and low latency – this is ideal for high-bandwidth applications that also require very fast ‘network response’, such as augmented and virtual reality, control of drones and robots, and control of manufacturing machine tools.

Higher bands, such as mmWave, do not propagate as far as lower-frequency bands, which sets up mmWave well for small cells and private wireless networks, especially indoors.

CBRS

In the U.S., the 150 MHz of CBRS (3.5 GHz) shared spectrum can be used by many different players, including mobile operators, cable operators, private LTE network providers for enterprises, and Wireless Internet Service Providers (WISPs). CBRS is ‘lightly licensed’ and is primarily being used for Private LTE and Private 5G networks, both indoor and outdoor. For example, it has been deployed outside in some communities to support remote K-12 learning during and after the pandemic.

CBRS supports both LTE and 5G. In February 2020, the OnGo Alliance completed Release 3 specifications, which support CBRS configurations for 5G New Radio (5G NR) and specify how to deploy a private network using both 3GPP LTE and 5G NR in the 3.5 GHz band.

Benefits of Private Wireless networks

While private 4G and 5G networks in the enterprise have been compared to Wi-Fi, there are additional benefits:

- Private cellular systems provide a predictable RF environment with better and more reliable coverage and capacity than Wi-Fi, generally speaking. Note that iGR does not think that private LTE/5G will supplant Wi-Fi any more than public LTE has. Wi-Fi and private LTE/5G are complementary.

- Private wireless networks may not need the involvement of an MNO to deploy but the private network can be connected to the public networks to enable roaming, etc.

- Deployed using the same 4G LTE and 5G network technology as public mobile networks use and hence benefit from technology developments and economies of scale.

- Efficient use of spectrum – private wireless networks using 4G LTE and 5G make very efficient use of the spectrum and can support connections of hundreds of megabits per second, if needed.

- Scalability – a private 4G LTE or 5G networks can be deployed with a single radio (cell) or hundreds, depending on the needs of the enterprise and application. Similarly, bandwidth from a few MB/s to hundreds of MB/s can be supported.

- Able to support new/emerging technologies, especially private networks using 5G – more accurate in-building location, IoT, augmented and virtual reality, etc.

- Provide customizable policy and network management features such as mobile settings and quality of service which are built into the LTE/5G standards.

- Highly secure, and the enterprise has complete control over its data. The 4G LTE and 5G air interfaces used in private networks are encrypted.

- Provides seamless mobility both intra-network (handoff of connections between cells) and inter-network (if the network connects to a public LTE network or to other private networks). Note that with dual SIM, dual standby and eSIM, one device can support both the private LTE network and a public LTE network.

- Support for neutral host, meaning that the private network can support multiple operators and still maintain the privacy and security of the various carriers/enterprises connected to the network.

- If using CBRS, the private LTE/5G ecosystem supports interoperability between suppliers and a Wi-Fi-like certification process for CBRS equipment and devices via the OnGo Alliance.

Drawbacks of Private Wireless Networks

Among the most cited negatives of deploying private networks are:

- Preparing the building or campus – this will vary by building/venue and by the type of network being installed but if more than a few cells are to be used, detailed network design and RF planning is usually required. Again, this comes down to cost.

- Operator trade-offs on where to best invest capital and operational dollars.

- As with any other wireless network, private 4G LTE and 5G networks can experience interference from other networks/sources. Interference reduces private network performance and capacity, which in turn can require higher investment/more sites to compensate if not mitigated.

- Cost of managing and operating a 4G LTE or 5G network – while the complexity of managing a private network has been reduced, these networks are more complicated and expensive to operate than Wi-Fi. That said, private networks can be deployed as a managed service, available from multiple vendors and providers.

Private wireless networks market size

Private wireless networks are a relatively new phenomenon and as such case studies and examples are relatively few. But the technologies are well understood and many enterprises, vendors, municipalities and organizations have deployed proof-of-concept and trial networks, with many more to come in the next few years.

iGR forecasts that the network spending (network equipment, installation and integration) opportunity in the U.S. just for CBRS will reach $5.1 billion in 2026. Globally, iGR estimates the private wireless network opportunity to be in excess of $9 billion in 2026. These estimates are only to deploy the private wireless networks and do not include the opportunity for developing and deploying new applications and services.

About iGR

iGR is a market strategy consultancy focused on the wireless and mobile communications and digital infrastructure industries. Founded in 2000 by Iain Gillott, one of the industry's leading analysts, iGR researches and analyzes the impact new wireless, mobile and digital infrastructure technologies will have on industries, the competitive landscape and on a company's strategic business plan.

A more complete profile of the company can be found at http://www.iGR - inc.com/.

Disclaimer

The opinions expressed in this market study are those of iGR and do not reflect the opinions of the companies or organizations referenced in this paper. All research was conducted exclusively and independently by iGR.