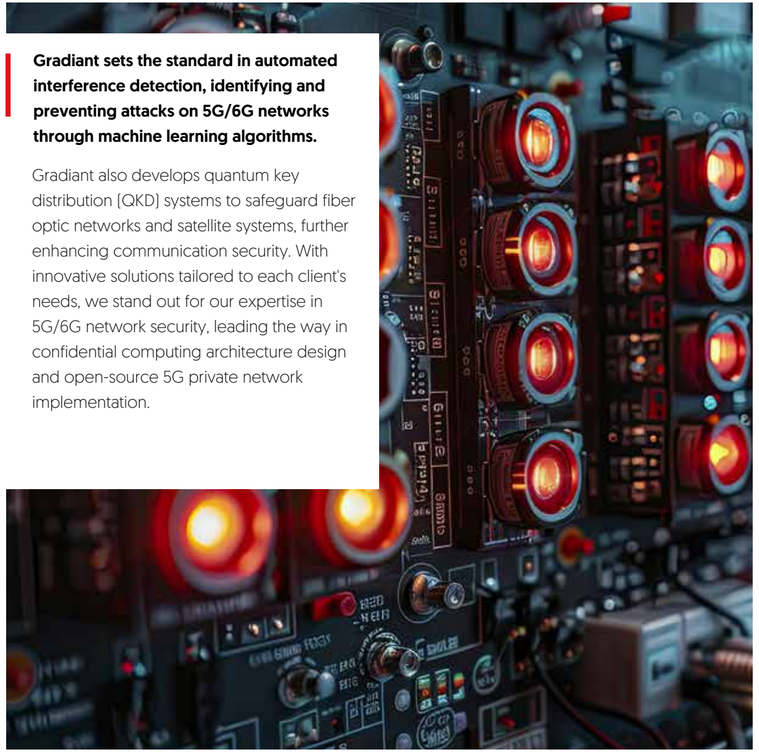
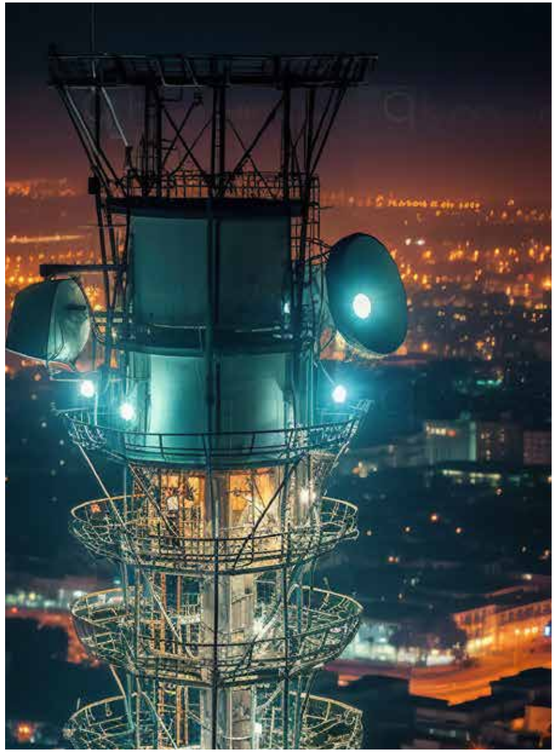


Gradiant sets the standard in automated interference detection, identifying and preventing attacks on 5G/6G networks through machine learning algorithms.

Gradiant also develops quantum key distribution (QKD) systems to safeguard fiber optic networks and satellite systems, further enhancing communication security. With innovative solutions tailored to each client's needs, we stand out for our expertise in 5G/6G network security, leading the way in confidential computing architecture design and open-source 5G private network implementation.

gradiant
Intelligence · Security
for your business

Estrada do Vilar, 56, 36214 Vigo, Pontevedra
(+34) 986 120 430 | gradiant@gradiant.org
www.gradiant.org



5G Mobile network security for industry

5G/6G & confidential computing solutions

gradiant

Setting the Standard: Expertise in 5G/6G Network Security & Confidential Computing Solutions

Automated interference detection

We can detect interfering radio signals, both intentional (inhibitors or jammers) and unintentional, using machine learning-based algorithms, which is crucial for ensuring security in 5G/6G networks.

For mobile operators, detecting and mitigating inhibition attacks block the reception of radio signals, resulting in a denial of service (DoS RAN) for users. In military Command and Control (C2) scenarios, inhibitors can disrupt communication between soldiers and command centers, jeopardizing operations.operations against inhibition attacks.

These solutions are ideal for managers of critical infrastructure with security or confidentiality requirements, such as prisons, nuclear power plants, airports, or technology parks.

Distributed spectral monitoring probe

In distributed radio access networks (RANs), we can create an interference map by detecting interference at different remote stations in the network. This approach encompasses both traditional distributed RANs and Open RANs, which allow for the installation of multiple radio points (probes) to detect interference and inhibitors.

For mobile operators and military applications, it's crucial not only to detect an inhibition attack but also to locate the source of the interfering signal, known as inhibitor geolocation. This enables the identification of the attacker's position and the suppression of the attack. It involves detecting signals (RF) at different points in the network, enabling the creation of a map to detect signals and determine their origin. An example of a potential use of this technology could be during the 2024 Paris Olympics.

5G Physical Layer Key Generation (PKG) control

PKG (Physical-layer Key Generation) is a technique that protects information directly at the physical layer by applying keys generated from the radio channel information between the two ends of communication. Currently, Gradiant is working on this type of keys in the millimeter and THz bands.

This approach has significant applications in mobile communication networks of operators. By integrating this encryption into their systems, end-users such as businesses could potentially dispense with additional security systems based on usernames and passwords.

Security based on Qtech

We are currently developing a quantum RF receiver capable of detecting interference. Unlike conventional detection methods, enabling us to mitigate interference across virtually any frequency used in communications.

We are also working in quantum key distribution (QKD) systems for implementation in fiber optic networks and satellite systems. The goal of QKD is to enable fiber optic link providers to protect these links using quantum technology. This approach is critical for both operator core networks and the fronthaul and backhaul of the radio access network (RAN).

5G private networks

In the connectivity realm, we've successfully rolled out a private 5G network in an industrial setting, providing connectivity to automated guided vehicles and other devices. Additionally, we've developed advanced tools for generating interference heatmaps in 5G networks and a channel model simulator.

We recently completed validation of the design and architecture of an eMBMS broadcast demonstrator, enabling simultaneous video reception on different terminal devices. Our capability to design and deploy private 5G networks in industrial environments offers network slicing capabilities to differentiate services, such as real-time machinery operation and autonomous vehicles.

Design of sensitive computing architectures

Gradiant excels in designing confidential computing architectures, including Multi Access Edge Computing (MEC), ensuring data and code confidentiality and integrity.

MEC reduces latency in services and applications by placing physical infrastructure closer to end-users. Confidential computing provides a solution by mitigating risks associated with this distributed infrastructure, ensuring that data and code remain protected.

Gradiant stands out for its ability to design and implement these solutions effectively, ensuring the security of networks and services.