Ericsson Technology Review

#2, February 2026

Jamming attacks in 5G wireless networks – detection and mitigation

Charting the future of innovation

Ericsson Technology Review – Charting the future of innovation | #2, February 2026

Jamming attacks in 5G wireless networks – detection and mitigation

Authors:
Henrik Forssell, Håkan Björkegren, Filippo Rebecchi, Harri Pietilä, Hugo Tullberg

Once considered a niche concern by many in the telecom industry, jamming has become a practical threat with real-world impact – one that network operators must be prepared to detect, localize and mitigate. 5G technology provides baseline resiliency against jamming and a robust platform for the creation of bespoke solutions tailored to different verticals, including those that deliver mission-critical and emergency communication services.

ISSN 0014-0171 284 23-3436 | Uen

Ericsson, SE-164 83 Stockholm, Sweden
Phone: +46 10 719 0000

Concerns about intentional network interference (jamming attacks) are rising as reliance on wireless networks continues to deepen and expand to include a growing number of private 5G networks with stringent security requirements.

To effectively address jamming threats, it is important to first understand what jamming entails, how it operates, and the ways in which it disrupts wireless communications. Signal jammers are devices that deliberately transmit electromagnetic interference to block or degrade the reception of legitimate wireless signals transmitted by everything from radio technologies used by wireless key fobs to Bluetooth, Wi-Fi, mobile networks (4G/5G) and global navigation satellite systems (GNSSs), including GPS, GLONASS and Galileo.

While they are illegal to operate, possess and sell in most countries [1,2], jammers are cheap and easy to acquire or build. The fact that they do not adhere to communication standards and spectrum regulations makes them difficult for receivers to handle and can result in significant disruption of services operating in both targeted and adjacent spectrum. In the mobile network context, jamming is primarily a radio access network (RAN) issue. This is because the 5G air interface uses a shared, publicly accessible radio medium, which means that anyone with the right equipment can transmit on it and potentially cause deliberate interference (jamming). The network's ability to automatically detect and respond to such incidents is critical to delivering the required levels of robustness and availability.

Jamming scenarios in mobile networks range from local criminal behavior – blocking connectivity for a small amount of user equipment (UE), for example – to coordinated attacks that deny service across a larger area. The impact can range from reduced quality of service to complete denial of service, depending on the jammer's power and proximity, as well as the network's configuration.

Overview of the threat landscape

The threat landscape for network operators is complex, as threat actors may target the enterprise business, the wireless service business and network subscribers in a variety of ways. A threat actor's objectives can range from financial (money) to informational (surveillance data or intellectual property, for example) to disruptive (from a technical or societal perspective) or downright destructive.

For example, criminals may want to disrupt mobile services during a bank robbery or burglary to prevent victims from calling for help and/or to interfere with police communication. Similarly, someone who is transporting stolen goods may want to disrupt mobile services for vehicle tracking. In some cases, private citizens choose to disrupt mobile services for personal reasons, such as disabling their children's internet access [3].

Terms and abbreviations

AoA – Angle of Arrival | **API** – Application Programming Interface | **DSSS** – Direct-Sequence Spread Spectrum | **FEC** – Forward Error Correction | **GLONASS** – Global Navigation Satellite System | **gNB** – Next Generation Node B | **GNSS** – Global Navigation Satellite System | **GPS** – Global Positioning System | **IQ** – In-phase and Quadrature | **LTE** – Long Term Evolution | **MCS** – Modulation and Coding Scheme | **MIMO** – Multiple-Input, Multiple-Output | **NR** – New Radio | **OFDM** – Orthogonal Frequency-Division Multiplexing | **PHY** – Physical Layer | **PDCCH** – Physical Downlink Control Channel | **PUCCH** – Physical Uplink Control Channel | **RAN** – Radio Access Network | **RU** – Radio Unit | **SC-FDMA** – Single-Carrier Frequency-Division Multiple Access | **SMO** – Security Management and Orchestration | **SSB** - Synchronization Signal Block | **TDD** – Time Division Duplex | **UE** – User Equipment | **3GPP** – 3rd Generation Partnership Project

Moreover, jammers targeting GNSS frequency bands are used to disable tracking for various reasons [4], including:

- fraud against fleet management or other tracking systems
- privacy concerns
- fraud against distance-based road user charging systems
- renting cars for trips outside the service area
- fraud against a distance-based vehicle insurance system.

In the future, we expect jammers to also target sensing capabilities of 6G networks.

The US Department of Homeland Security has warned that the smuggling of jammers across borders has increased significantly since 2021 [5]. Furthermore, The Finnish Transport and Communications Agency has reported that it found 714 personal GNSS jamming devices on the roads in 2023, a significant rise from 2022 [6].

Jammer characteristics and methods of operation

Jammers come in various sizes, support the jamming of different bands simultaneously, can be battery or externally powered and vary in output power and range. The main methods of operation of jammers are:

- narrowband jamming, where the energy is concentrated on a narrow frequency band
- wideband sweep jamming, where narrowband interference rapidly moves across a wide frequency range
- barrage jamming, where the energy is spread over the frequency range.

A typical battery-powered handheld jammer has an output power of 1W per band but externally-powered jammers can provide up to 10W per band or even higher. Commercial jammers can jam 2G, 3G, 4G and even 5G bands with different versions for US and European markets. They can also jam GPS, Wi-Fi, car remote control devices and much more.

Sweep signals are widely used by commercial jammers. **Figure 1** provides an example of a wideband sweep jammer captured in the uplink bands (LTE B20 and B8) by an Ericsson radio, illustrating the received uplink spectrum snapshots over time before and during the jamming event. A significant change in the received power spectral density and increased received power can be observed as the jamming event starts after approximately 50 minutes.

4G LTE and 5G New Radio jamming

In addition to indiscriminate sweep or barrage jamming, mobile 4G and 5G services can be disrupted by attack vectors that target specific radio resources [7], such as:

- synchronization signals
- broadcast channels
- control channels
- data-plane channels
- reference signals.

Synchronization signals – the primary synchronization signal and the secondary synchronization signal for 4G and the synchronization signal block (SSB) for 5G – can be jammed with the intention to block cell detection and disrupt time/frequency synchronization, preventing new connections and causing loss of active connections. 5G NR's flexible SSB placement across bandwidth makes it harder to target than 4G LTE's fixed SSB allocation.

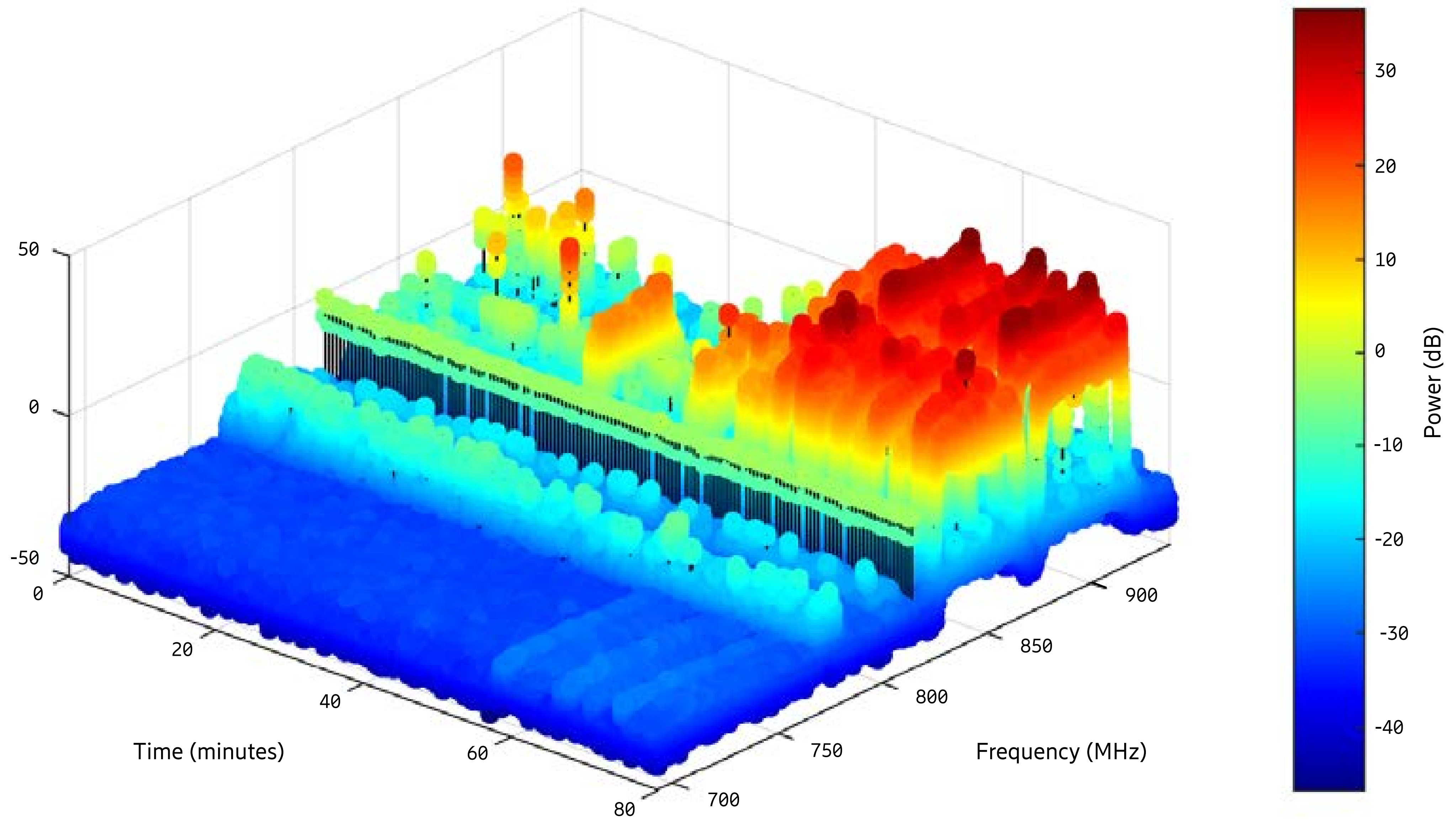

Figure 1: Spectrum measurements from an Ericsson radio showing a wideband sweep jammer

Jamming of the physical broadcast channel prevents new UE attachments, which means that new connections cannot be established. 5G NR broadcasts less information than 4G LTE, reducing interception and abuse risks. In 4G LTE it takes little effort to jam the physical control format indicator channel, which can severely degrade control-plane operation [8]. In 5G NR this channel has been replaced with a flexible control architecture carried on the physical downlink control channel (PDCCH), which makes the NR control plane more resilient against jamming.

Both PDCCH and physical uplink control channel (PUCCH) jamming can degrade control-plane operations. The PUCCH is particularly vulnerable, but 5G NR's dynamic time/frequency mapping makes jamming on the edges of the uplink bandwidth less effective than it was in 4G LTE.

Jamming of the data-plane channels (physical downlink shared channel and physical uplink shared channel) increases data error rates by corrupting symbol demodulation, leading to reduced or unavailable service. The data-plane channels occupy the largest portion of time-frequency resources and can be attacked either via narrow or wideband attacks.

> Beamforming with Massive MIMO has emerged as a resilient technology against jamming.

Reference signal (demodulation reference signal, channel state information reference signal and sounding reference signal) jamming disrupts channel estimation and multiple-input, multiple-output (MIMO) beamforming accuracy. This leads to corrupted data demodulation, a decline in data-plane quality and degradation in MIMO and beamforming performance.

In addition, jamming that targets GNSS frequencies can indirectly impact RAN performance in cases where GNSS is used for time and frequency synchronization. Short disturbances can be mitigated by holdovers up to a few hours for a time division duplex (TDD) base station [8]. Further resilience can be achieved by having multiple distributed (based on precision time protocol) synchronization sources and a combination of GNSS and ground-based clocks.

5G New Radio resilience against jamming

Traditionally, the primary countermeasure against jamming has been the use of spread-spectrum techniques, which distribute the communication signal over a wide frequency range. Classical approaches include:

- direct-sequence spread spectrum (DSSS), which uses a high-rate pseudo-random code to spread the signal across many narrowband frequencies
- frequency-hopping spread spectrum, which rapidly changes the carrier frequency according to a pseudo-random pattern.

These methods force an adversary to jam a much larger portion of the spectrum. Additional mitigation techniques include forward error correction (FEC), adaptive modulation and coding, hybrid automatic repeat request, pseudo-random scrambling and channel interleaving. These latter techniques are all part of standard 3GPP methods for reducing error rates due to varying interference and channel conditions.

More recently, beamforming implemented with Massive MIMO has emerged as a resilient technology against jamming: by exploiting channel state information and spatial diversity, beamforming can concentrate energy on intended receivers and nullify or mitigate interferers; its effectiveness increases with the number of antenna elements. All of these techniques, with the exception of fast frequency hopping, are available in 5G NR.

In 5G, the primary multiple access schemes are based on orthogonal frequency-division multiple access for the downlink and single-carrier frequency-division multiple access (SC-FDMA) for the uplink, offering higher spectral efficiency. Orthogonal frequency-division multiplexing (OFDM) effectively utilizes the available wide frequency channel by modulating data over many narrow, orthogonal subcarriers. When combined with error-correcting coding across subcarriers, it provides a spreading effect that enhances resilience against jamming, similar to DSSS.
In the uplink, SC-FDMA also contributes to spreading by employing a larger frequency allocation than the data rate requires, effectively lowering the FEC code rate. Additionally, spread-spectrum principles remain in use for key synchronization and reference signals in 5G. This spreading gain enables communication links to operate under challenging conditions, such as with signal-to-interference-plus-noise ratios well below -6dB for low data rates.

Interference-aware scheduling evaluates radio resources at each scheduling interval (typically 1ms) and preferentially allocates resources that exhibit lower levels of jamming or interference. Deploying multiple frequency bands further enhances robustness by enabling the scheduler to select bands that are less affected by jamming. Effectively, this enables relatively slow frequency hopping for data. However, control channels are not particularly flexible; to some extent the control signaling can be reconfigured but only on a much slower basis. Collectively, these measures form a robust baseline defense against jamming, which is fundamentally a form of intentional interference.

The ability to detect ongoing jamming attacks can be used to further improve mitigation during operation. Once a jamming attempt is detected, the network can evade interference by dynamically reconfiguring parameters such as frequency bands, modulation schemes, MIMO configurations, system load and transmission power. Advanced algorithms can analyze the jamming signal's characteristics to predict future patterns and enable proactive countermeasures. For example, identifying the jammer prevents UE in affected cells from raising their transmission power, limiting the jamming impact to devices near the source. Similarly, by reducing load in regions close to the jammer, the network can preserve the integrity and resilience of the broader cellular system.

Detection and positioning of jamming in the radio access network

In today's mobile networks, high-level performance management counters provide coarse indicators of abnormal interference. Typical metrics include signal-to-noise ratios, reference signal received quality and automatic gain control levels measured and aggregated by base stations.

While useful as high-level indicators of jamming, these metrics are designed for long-term performance monitoring (from days to months) and are less suited for detection of sudden onsets, such as the start of a jamming event. Mission-critical networks may have tighter requirements on time-to-detect (within 500ms of the onset of the attack, for example). Such scenarios require local detection algorithms that process physical layer signals such as baseband in-phase and quadrature (IQ) samples.

Signal and spectrum analysis for detection and localization

Signal-based jamming detection algorithms fit into one of two categories: anomaly detection and signature-based detection. Anomaly detection algorithms learn the normal behavior of IQ signals (typical OFDM patterns in 5G NR, for example) and flag deviations. Signature-based algorithms

> The ability to detect ongoing jamming attacks can be used to further improve mitigation during operation.

search for components with specific characteristics such as periodic waveforms or specific statistical distributions. Anomaly detection commonly uses an autoencoder or temporal convolutional models trained on normal 5G NR OFDM signals. Typically, such models are trained to reconstruct received signals from a low-dimensional representation, where deviations from the normal behavior can be detected based on large reconstruction errors.

Signature-based algorithms rely on statistical classification of spectral and time-frequency traits of the received signals. Examples include detecting periodic signal components (such as wideband sweep jammers) using autocorrelation or detecting constant-envelope signals. These algorithms can also be used to classify the type of jammer or even identify the specific device characteristics.

Since real-world jamming transmitters are diverse in terms of the waveforms they emit, practical solutions combine anomaly- and signature-based algorithms and allow new signatures to be added over time.

The 5G New Radio air interface uses multiple effective techniques to combat unintentional interference and intentional jamming.

Once a detection is confirmed, additional methods can be used to coarsely geolocate the jamming transmitter. The options depend on the RAN deployment: with Massive MIMO radios, the Angle of Arrival (AoA) estimation (using methods such as multiple signal classification, for example) can estimate the jammer direction or location using multiple radios. In sparser deployments, localization can rely on differential power at multiple sites or simply identifying the most likely site or sector.

All of these techniques consume uplink IQ signals and, depending on the system configuration (TDD or frequency division duplex), may not detect downlink jamming. While uplink jamming is arguably more critical, as 5G NR is more sensitive to uplink jamming [9], downlink jamming can be detected using standardized 5G UE measurement reports [10] and potential new UE measurements in 6G [11].

Data collection for jamming detection

Designing RAN solutions for jamming detection that operate on IQ signals poses challenges for both data collection and algorithm runtime environments. For reference, the IQ samples on a single 5G NR carrier with 50MHz bandwidth and 30kHz subcarrier spacing amount to a front-haul data rate of roughly 2Gbps per antenna stream. In a network with multiple sites, sectors and antennas, centralized collection and processing of all IQ data quickly becomes infeasible.

Techniques for overcoming this problem are selective or randomized sampling and offloading of detection to local RAN compute such as in the radio unit (RU), distributed unit or edge compute. Ericsson radios support a feature that allows remote monitoring of the IQ signal and radio frequency spectrum. This feature can be manually triggered or scheduled to collect small snapshots of IQ samples at regular intervals and can serve as a data source for jamming detection use cases.

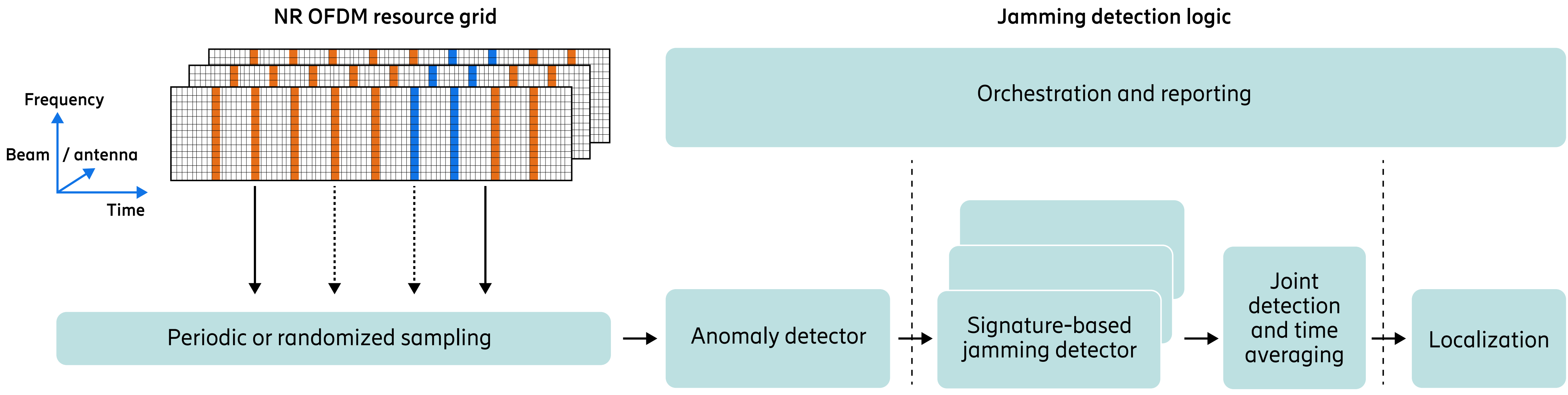
NR OFDM resource grid
Jamming detection logic
Frequency
Beam
/ antenna
Time
Orchestration and reporting
Periodic or randomized sampling
Anomaly detector
Signature-based jamming detector
Joint detection and time averaging
Localization

Figure 2: Jamming detection logic based on periodic or randomized sampling of IQ samples from the uplink OFDM resource grid

Future jamming detection solutions may require even more flexible sampling of IQ data, as illustrated in **Figure 2**, where only a selected subset of the IQ data is processed by the detection algorithms. Anomaly detection is performed as a first step, so that signature-based algorithms only consume processing resources once an anomaly is detected. The results from multiple detectors are combined to confirm the detection and perform localization. An initial selection can be performed using local logic based on performance metrics, followed by selective sampling of IQ samples across carriers, MIMO layers and time-frequency resources. Pseudo-random sampling can further improve robustness against smart jammers that attempt to evade deterministic sampling strategies.

Ensuring resilience against jamming

Building a resilient network requires combining architectural principles with operational capabilities. At a minimum, designing and operating a network that is resilient against jamming requires:

- threat intelligence on likely actors, motives and available jamming techniques and devices
- a resilient air interface by design that utilizes spatial, time and frequency diversity, and includes interference mitigation features
- secure and robust deployment, configuration and synchronization of the network.

For mission-critical use cases, additional layers of protection may be necessary, such as:

- security monitoring and detection systems that can detect and, where possible, geolocate jamming based on data collected from the base stations.
- automated response that adapts network configuration based on detection

- exposure of detection insights to trusted third parties through external RAN interfaces
- use of geolocation information to support the apprehension of perpetrators and seizure of jamming devices.

These capabilities are particularly relevant for mission-critical services within government, defense, enterprise, health care, public safety and power systems, where custom jamming solutions allow the RAN to inform operators and public authorities about ongoing incidents. For example, a national power grid operator could subscribe to detection metrics from nearby 5G base stations to receive early warnings on communication and synchronization problems, while a truck logistics company could receive alerts on GNSS outages along planned routes.

Figure 3 illustrates the RAN architecture with functionality for jamming detection, localization and mitigation labeled with the letters A, B, C and D. The letter A highlights the resilient air interface, which is deployed in the lower/upper physical layer (PHY). The air interface utilizes spatial, time and frequency diversity to mitigate the impact of jamming interference. Adaptive modulation and coding schemes (MCSs), frequency hopping, FEC and MIMO beamforming are applied.

Future jamming detection solutions may require even more flexible sampling of IQ data.

The letter B highlights local jamming detection and the geolocalization of jamming signals in or near the base station. Interference key performance indicators are used to trigger IQ signal-level detection algorithms. Estimation of the AoA and signal power can be used for coarse source localization. Detection and localization algorithms can either run in the gNB baseband or in local edge compute depending on the deployment.

The letter C highlights local jamming mitigation actions deployed across the PHY, the medium access control and radio resource control layers (layers 1-3 in the figure), such as prioritization of robust MCSs, resource scheduling on non-jammed physical resource blocks and handover to a non-jammed carrier.

Finally, the letter D highlights security management and orchestration (SMO), which includes reporting based on centralized management of detection events collected from the base stations and analysis of spectrum measurements from the RU. SMO also includes localizing jammer signals, tracking their movement, providing alerts about new jamming events and proposing mitigation actions.

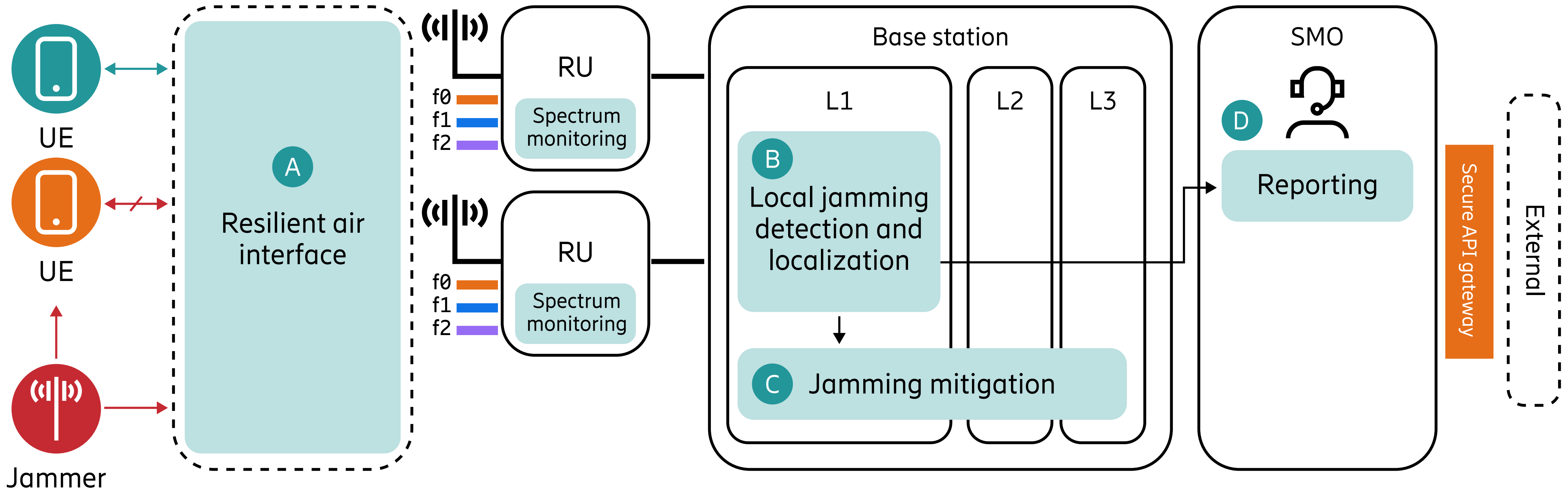

Figure 3: RAN architecture highlighting functionality for jamming detection, localization and mitigation

Conclusion

As the threat landscape for critical infrastructure and mobile networks continues to evolve, resilience against jamming is of growing importance. In this article, we have outlined the existing jamming threats to mobile networks and their current and potential future capabilities for detecting, locating and mitigating jamming attacks in the radio access network (RAN).

The 5G New Radio (NR) air interface utilizes multiple effective techniques to combat both unintentional interference and intentional jamming. The combination of orthogonal frequency-division multiplexing (OFDM), advanced error-correcting coding, massive multiple-input, multiple-output (MIMO) beamforming, interference-aware scheduling and sophisticated interference-suppression algorithms implemented in both the 5G base station and the user equipment provides 5G NR with substantial resilience against jamming and other hostile interference. The effectiveness of such techniques will, in practice, depend on the various parameters like transmit power and scale and sophistication of the attack. To further enhance the resilience of RANs, knowledge of the existing jamming threats is necessary in both system design and standardization, as well as robust deployment and configuration of the network.

Certain deployments of 5G and future 6G networks – such as mission-critical networks and defense, health care and enterprise networks – would benefit from custom jamming detection and mitigation solutions. Moreover, trusted external entities like power-grid operators, law enforcement and defense may benefit from using the existing RAN infrastructure to do spectrum monitoring and jamming detection in sensitive areas. In this article, we have highlighted the possibilities of designing such solutions where the key enablers are flexible extraction of PHY layer data from the base stations and a combination of anomaly detection and signature-based jamming detection algorithms.

The authors

Henrik Forssell is a signal processing researcher at Business Area Networks. He joined Ericsson in 2021. His work focuses on product-near development and proof-of-concept solutions for air-interface security and artificial intelligence/machine learning for the physical layer and positioning. Forssell holds a Ph.D. in electrical engineering from KTH Royal Institute of Technology in Stockholm, Sweden.

Håkan Björkegren is a principal researcher at Ericsson Research who joined the company in 1995. During his career, he has worked on signal processing and air-interface aspects for 2G-6G, DAB, Bluetooth, sensing and security. Björkegren holds a Ph.D. in signal processing from Luleå University of Technology in Sweden.

Filippo Rebecchi is a researcher in concepts security within Business Area Networks. He joined Ericsson in 2022. His current focus is on advancing security technologies and their application to RAN architectures. Rebecchi holds a Ph.D. in networking and telecommunications from UPMC Sorbonne University, Paris, France.

Harri Pietilä is the director of threat intelligence and cyber defense at Ericsson Security Solutions. He joined the company in 2014. Pietilä has worked on solutions to counter threats to mobile networks for several years and is currently focusing on threats in the wireless airspace, such as false base stations and jamming. He holds a Ph.D. in astronomy and an M.Sc. in theoretical physics from the University of Turku, Finland.

Hugo Tullberg is a principal researcher at Ericsson Research. He joined Ericsson in 2021. His research interests include information and coding theory, artificial intelligence, machine learning and network resilience. He is currently working on air-interface resilience. Tullberg holds a Ph.D. in electrical and computer engineering from the University of California San Diego, USA.

References

1. United States Federal Communications Commission, Jammer Enforcement, April 2020 ↗
2. European Commission, Guide to the Radio Equipment Directive 2014/53/EU, December 19, 2018 ↗
3. Bitdefender, French dad uses signal jammer to stop his kids from going online, takes down neighborhood's internet too, February 18, 2022 ↗
4. GPSPATRON, In-Car Jammers are Killing GNSS Integrity, January 18, 2022 ↗
5. U.S. Department of Homeland Security press release, Homeland Security Warns about the Spike in China-Based Technology Firms' Smuggling of Signal Jammers, June 18, 2025 ↗
6. Yle, Finland detects more GPS jammers as drivers increasingly try to hide their tracks, March 12, 2024 ↗
7. IEEE Xplore, 2018 IEEE International Conference on Communications Workshops (ICC Workshops), Kansas City, MO, USA, 2018, pp. 1-6, doi: 10.1109/ICCW.2018.8403769, 5G NR Jamming, Spoofing and Sniffing: Threat Assessment and Mitigation, Lichtman, M.; Rao, R.; Marojevic, V.; Reed, J.; and Jover, R.P. ↗
8. Ericsson Technology Review, 5G synchronization requirements and solutions, January 13, 2021, Ruffini, S.; Johansson, M.; Pohlman, B.; Sandgren, M ↗
9. FFI (The Norwegian Defence Research Establishment) report, A study of 5G New Radio and its vulnerability to jamming, April 27, 2022 ↗
10. IEEE Xplore, 2023 IEEE International Conference on Communications, Rome, Italy, 2023, pp. 5216-5220, doi: 10.1109/ICC45041.2023.10279513, UE-Assisted Jamming Detection in 5G NR, Forssell, H.; Mungara, R. K.; Ferrante, G. C.; and Tullberg, H ↗
11. Ericsson blog, 6G RAN – key building blocks for new 6G radio access networks, May 15, 2024, Parkvall, S.; Wiemann, H ↗

Further reading

- 5G security – enabling a trustworthy 5G system ↗
- Safeguarding telecom networks against advanced threats with Ericsson's cyber defense solutions ↗
- Transforming the future of defense digitalization ↗
- Ericsson Uplink Anomaly Detector rApp ↗
- Telecom security ↗
- Security management for a new era ↗
- Exploring the evolution of RAN security management ↗
- Unifying threat modeling and hunting at runtime for proactive cyber defense ↗