TRANSNAV the International Journal on Marine Navigation and Safety of Sea Transportation
http://www.transnav.eu
Volume 20
Number 2
June 2026

DOI: 10.12716/1001.20.02.09

GNSS Jamming and Spoofing Situational Awareness Maps

D. Zmysłowski & J.M. Kelner
Military University of Technology, Warsaw, Poland

ABSTRACT: The widespread and rich use of global navigation satellite systems (GNSSs) means that they have become a frequent target for intentional interference that impedes, falsifies, or prevents their operational existence. Such activities are related to deliberate disinformation actions or limiting access to services essential for transport, critical infrastructure, government, civil services, or military. They are usually an element of asymmetric hybrid actions carried out as part of information warfare conducted in the electromagnetic spectrum using electronic warfare (EW) techniques, terrorist operations, or are related to human carelessness. In military operations, they constitute a means of influencing navigation warfare (NAVWAR). When GNSS is caused by jamming or spoofing, it becomes challenging to use effectively. Utilizing their services introduces significant uncertainty, as it is unclear whether the provided values for position, speed, and time are reliable. Nowadays, many incidents are observed concerning the jamming of GNSS signals, causing adverse effects on maritime navigation, air operations, and land transport, the synchronization of telecommunications systems (especially mobile), as well as disruptions to the operation of energy and financial systems. The scale of these phenomena is massive, and their scope covers countries (e.g., Ukraine), regions of countries (e.g., Poland, Lithuania, Latvia, Estonia, Finland, Sweden, and others), also large areas of shipping waters, such as the Baltic Sea, the Mediterranean Sea, or the Black Sea. In this paper, we present the idea of using situational awareness maps to visualize and assess the current state of disruptions to the functioning of global systems in each region caused by jamming or spoofing.

1 INTRODUCTION

Global navigation satellite systems (GNSSs) constitute a fundamental component of modern positioning, navigation, and timing (PNT) infrastructures. They underpin a wide spectrum of civilian and military applications, including aviation and maritime navigation, land transportation, telecommunications and financing sector synchronization, power-grid monitoring, and precision-guided military operations. The ubiquitous reliance on GNSS-derived PNT information has, however, exposed a critical vulnerability: the extreme susceptibility of GNSS signals to intentional and unintentional radio-frequency (RF) interference [1].

GNSS signals received at the Earth's surface are characterized by very low power levels, typically well below the thermal noise floor. As a result, even low-cost and low-power transmitters are capable of significantly degrading GNSS reception. Among intentional interference methods, jamming and spoofing represent the most serious and operationally relevant threats. Jamming aims to deny GNSS service by overwhelming receivers with interference, while spoofing seeks to deceive receivers by broadcasting

counterfeit navigation signals, potentially inducing hazardous position or timing errors without immediate detection [2], [3], [4], [5].

In recent years, the operational relevance of GNSS interference has increased markedly due to the proliferation of portable jammers, software-defined radios (SDRs), and increasingly sophisticated spoofing techniques. This evolution has elevated GNSS interference from a localized nuisance to a strategic instrument within the broader framework of navigation warfare (NAVWAR) [6], [7]. In military contexts, GNSS disruption can directly impair command and control, precision fires, unmanned systems, and synchronized communications. In civilian domains, documented interference incidents have demonstrated their capacity to affect airport operations, maritime safety, emergency services, and other elements of critical infrastructure.

Ensuring resilience against such threats requires more than robust receiver design alone. It necessitates the ability to observe, interpret, and respond to the dynamic GNSS interference environment in near real time. This capability is commonly referred to as GNSS situational awareness (GNSS-SA) [8], [9]. GNSS-SA encompasses the continuous monitoring of GNSS signal performance and integrity, the detection and classification of anomalies, and the contextual interpretation of these observations within an operational and geographic framework.

A key enabler of GNSS-SA is the GNSS situational awareness map (GNSS-SAM). GNSS-SAM can be understood as a dynamic, georeferenced visualization environment that integrates heterogeneous GNSS performance metrics and interference indicators collected from distributed sensor networks. By fusing data from reference GNSS stations, mobile platforms, specialized interference monitoring sensors, and crowd-sourced receivers, GNSS-SAM provides a spatially coherent representation of GNSS service quality and threat conditions. This map-based paradigm transforms raw signal-level measurements into actionable situational awareness products, supporting timely mitigation actions and informed operational decision-making.

The objective of this paper is to present a comprehensive overview of GNSS jamming and spoofing situational awareness maps, with particular emphasis on the GNSS-SAM concept. The paper discusses the architectural foundations and functional objectives of GNSS-SAM systems, the data sources and signal-level features used for interference detection and classification, and the role of data fusion and geospatial visualization in enhancing situational awareness. Selected application scenarios from aviation, maritime operations, telecommunications, and security and defense domains are examined to illustrate the operational value of GNSS-SAM-based approaches.

Several GNSS-SA–oriented solutions have already been proposed in the literature; however, these approaches typically address only selected aspects of the overall problem and do not provide a fully integrated, multi-layer situational awareness framework. For example, aerial mapping solutions based on unmanned aerial vehicles have been demonstrated as effective tools for detecting and localizing GNSS interference sources over large areas, offering high spatial resolution and flexibility, but they are inherently episodic and platform-dependent rather than continuously operating monitoring systems [10]. Crowdsourcing-based approaches leveraging smartphone applications have shown promise in enabling large-scale, real-time mapping of GNSS interference with minimal infrastructure cost; nevertheless, such methods are constrained by heterogeneous receiver quality, limited signal observables, and reduced detection reliability [11].

More comprehensive monitoring services, such as national GNSS-SA platforms based on permanent reference station networks, can provide continuous signal quality assessment and leverage advanced services such as Galileo Open Service Navigation Message Authentication (OSNMA) and the High Accuracy Service (HAS). The Finnish Geospatial Research Institute (FGI) has implemented an open-access GNSS-SA platform, referred to as GNSS-Finland, which provides continuous monitoring of GNSS signal conditions. The system assesses signal quality, identifies indications of interference, and delivers information on the anticipated performance of GNSS services based on observations from approximately 47 stations belonging to the Finnish continuously operating reference station (CORS) network. However, these systems remain geographically limited and are often tailored to specific constellations or services rather than addressing GNSS interference awareness in a fully global and multi-domain sense [12]. These examples highlight the need for a more holistic GNSS-SAM concept capable of integrating heterogeneous data sources, detection techniques, and visualization layers into a unified operational picture.

By consolidating existing concepts and practical solutions into a coherent framework, this work aims to contribute to the development of resilient GNSS monitoring, interference awareness, and navigation assurance strategies applicable to both civilian and military environments.

The main contribution of this paper is the introduction of a unified GNSS-SAM conceptual framework integrating heterogeneous sensor networks, interference indicators, geospatial visualization techniques, and operational awareness mechanisms into a coherent architecture supporting resilient PNT monitoring.

The remainder of this paper is organized as follows. Section 2 discusses the inherent vulnerabilities of GNSS and the principal interference threats arising from jamming and spoofing. Section 3 introduces the concept of GNSS SA and defines the role of the GNSS SAM. Section 4 outlines the key objectives and functional requirements of GNSS SAM systems, while Section 5 describes the data sources and sensor networks supporting GNSS SAM operation. Section 6 focuses on signal features and interference indicators, and Section 7 presents data fusion and anomaly classification approaches applied within GNSS SAM frameworks. Section 8 addresses geospatial visualization aspects and overall GNSS SAM architecture. Section 9 reviews existing GNSS SAM solutions, and Section 10 discusses representative application scenarios. Section 11 provides a discussion

of current challenges and future development directions, and Section 12 concludes the paper.

2 GNSS VULNERABILITIES AND INTERFERENCE THREATS

2.1 *Characteristics of GNSS Signals and Inherent Vulnerabilities*

GNSSs are based on the reception of spread-spectrum radio signals transmitted by satellites operating at medium Earth orbit altitudes of approximately 20,000 km. Due to the long propagation distance and limited satellite transmit power, GNSS signals arrive at the user receiver with extremely low power levels, typically on the order of −160 dBW to −130 dBW. These signal levels are often well below the thermal noise floor of the receiver front end, requiring sophisticated correlation and integration techniques for reliable signal acquisition and tracking [1].

This fundamental signal weakness constitutes the primary source of GNSS vulnerability. Any additional radio-frequency energy present within the GNSS bands, whether unintentional or deliberate, can significantly degrade receiver performance. Even narrowband interference affecting only a small portion of the spectrum may disrupt code or carrier tracking loops, leading to loss of lock, increased measurement noise, or biased pseudo-range estimates. The reliance on open, publicly documented signal structures further amplifies the exposure of civil GNSS signals to exploitation [13], [14].

Moreover, GNSS receivers typically operate under the assumption of benign signal environments. While modern receivers incorporate interference mitigation features, many mass-market and legacy systems lack robust detection mechanisms for sophisticated threats. As a result, performance degradation may remain unnoticed until navigation or timing errors reach operationally critical levels. These inherent vulnerabilities form the technical foundation upon which both jamming and spoofing attacks are built [13], [15].

2.2 *Jamming Techniques and Effects*

GNSS jamming refers to the intentional transmission of RF signals designed to disrupt the reception of legitimate GNSS signals. The simplest form of jamming employs continuous-wave (CW) interference centered on a GNSS carrier frequency. Despite its simplicity, CW jamming can be highly effective, particularly against receivers with limited front-end filtering or adaptive notch capabilities. More advanced jammers employ broadband or chirp-like waveforms to cover wider frequency ranges and affect multiple GNSS constellations simultaneously [4], [16].

From an operational perspective, jamming primarily results in denial-of-service attacks. Receivers exposed to sufficiently strong interference experience a rapid reduction in carrier-to-noise density ratio (C/N_0), followed by loss of satellite tracking and invalid navigation solutions [17], [18]. Timing receivers may experience holdover mode activation or, in severe cases, complete loss of synchronization. As highlighted in the presentation material, sudden C/N_0 drops exceeding 10 dB across multiple receivers represent a strong indicator of jamming activity [15].

Jamming attacks are particularly attractive due to their low technical barrier and cost-effectiveness. Portable jammers, often powered by vehicle batteries, can create disruption zones spanning several kilometers, especially in open environments such as maritime or rural areas. While jamming is relatively easy to detect, its mitigation remains challenging in real time, reinforcing the need for distributed monitoring and situational awareness mechanisms such as GNSS-SAM systems [11].

2.3 *Spoofing Techniques and Threat Scenarios*

In contrast to jamming, GNSS spoofing aims not to deny service, but to manipulate receiver outputs by transmitting counterfeit GNSS-like signals. These signals are structured to mimic authentic satellite signals while conveying false navigation data. Spoofing attacks range from simple meaconing (rebroadcasting delayed genuine signals) to highly sophisticated seamless spoofing, where the victim receiver is gradually captured without loss of lock [4], [19], [20].

Spoofing poses a particularly dangerous threat because it can remain covert. A receiver under spoofing attack may continue to report valid position and time solutions that appear internally consistent, while being significantly offset from reality. In timing-dependent infrastructures such as telecommunications networks or power grids, even microsecond-level timing offsets can lead to cascading failures or loss of synchronization [21].

Detection of spoofing typically relies on indirect indicators rather than raw signal power levels. As discussed in the presentation, such indicators include inconsistencies between satellite elevation and azimuth angles, correlation function distortions, time-jump events, and multi-receiver spatial inconsistencies. The complexity and subtlety of spoofing attacks make them a central concern for GNSS-SA frameworks and motivate the integration of multi-sensor and map-based analysis tools [5], [20], [22], [23].

2.4 *Operational Impact of GNSS Interference*

The operational consequences of GNSS interference extend far beyond isolated receiver failures. In aviation, jamming and spoofing events near airports can disrupt GNSS-based approach procedures and increase pilot workload, potentially leading to flight delays or diversions. Maritime operations face similar risks, particularly in congested ports and narrow waterways where precise positioning is essential for safe maneuvering [24], [25], [26], [27].

In terrestrial and infrastructure domains, GNSS interference can compromise synchronization in cellular networks [28], [29], [30] and power grids [21], [31]. Telecommunications base stations relying on GNSS timing may experience phase misalignment, leading to degraded service quality or network outages. Power systems using phasor measurement units (PMUs) are particularly sensitive to timing errors,

which can undermine grid stability during dynamic operating conditions [32], [33].

From a military perspective, GNSS interference is an integral element of NAVWAR [6], [7]. Disrupting GNSS-based PNT can degrade command and control, precision-guided munitions, unmanned systems, and coordinated maneuvers. These wide-ranging impacts underscore the necessity of continuous, geospatially aware monitoring solutions capable of correlating interference effects across domains, precisely the role envisioned for GNSS-SAM architectures.

3 GNSS SITUATIONAL AWARENESS CONCEPT

3.1 *Definition of GNSS Situational Awareness (GNSS SA)*

GNSS-SA can be broadly understood as the capability to perceive, comprehend, and anticipate the operational state of GNSS services within a given spatial and temporal context. Unlike traditional performance monitoring, which focuses primarily on receiver-level metrics, GNSS-SA emphasizes system-level understanding by correlating observations from multiple sensors and platforms. This holistic perspective is essential in environments where GNSS signals are subject to dynamic interference, intentional attacks, or environmental disturbances.

At its core, GNSS-SA builds upon continuous observation of GNSS signal characteristics such as C/N_0, tracking stability, pseudo-range consistency, and timing integrity. However, raw measurements alone are insufficient to provide meaningful awareness. GNSS-SA requires contextualization of these measurements, including knowledge of the receiver location, satellite geometry, operational environment, and temporal evolution of observed anomalies. Only through such contextual integration can deviations from nominal behavior be correctly interpreted.

An important aspect of GNSS-SA is its ability to discriminate between benign degradations and hostile actions. Natural phenomena such as ionospheric scintillation, multipath in urban environments, or satellite maintenance events may produce symptoms similar to deliberate interference. Therefore, GNSS-SA frameworks rely on comparative analysis across geographically distributed sensors to identify patterns that are inconsistent with natural causes, such as abrupt spatial boundaries or simultaneous multi-frequency disruptions.

Finally, GNSS-SA should be viewed as a decision-support capability rather than a standalone detection mechanism. Its ultimate purpose is to enable timely and informed responses, such as switching to alternative navigation or timing sources, issuing operational warnings, or initiating countermeasures. This aligns GNSS-SA conceptually with situational awareness paradigms used in air traffic management, maritime domain awareness, and cybersecurity operations [9].

3.2 *GNSS Situational Awareness Map (GNSS SAM): Definition and Scope*

The GNSS-SAM represents a practical and intuitive realization of the GNSS-SA concept. GNSS-SAM can be defined as a dynamic, georeferenced dashboard that integrates heterogeneous GNSS performance data (i.e., signal metrics, interference reports, integrity monitors) from distributed sensor nodes, processes these data through analytics and anomaly-detection algorithms, and presents them as layered geographic information for decision-makers to assess and respond to GNSS threats or degradations. By projecting these data onto a geographic map, GNSS-SAM enables operators to rapidly assess the spatial extent, severity, and evolution of GNSS degradations.

In contrast to conventional dashboards or tabular monitoring tools, GNSS-SAM leverages spatial cognition to enhance human understanding of complex interference scenarios. Color-coded performance layers, event markers, and temporal animations allow users to identify interference 'hotspots,' movement of jamming sources, or regions affected by spoofing. This spatial abstraction is particularly valuable when monitoring wide-area infrastructures such as airspace sectors, maritime regions, or national communication networks.

The scope of GNSS-SAM extends beyond real-time visualization. As emphasized in the presentation, GNSS-SAM systems typically incorporate historical data archiving, enabling post-event forensic analysis and long-term trend assessment. Such capabilities support the identification of recurring interference patterns, assessment of adversary tactics, and evaluation of mitigation effectiveness. In this sense, GNSS-SAM functions both as an operational tool and as an analytical platform.

It is also important to note that GNSS-SAM is inherently scalable. Depending on the application, it may operate at local, regional, or global levels, integrating data from a handful of specialized sensors or thousands of heterogeneous receivers. This flexibility allows GNSS-SAM architectures to be adapted to diverse civilian and military use cases, from port-level monitoring to national or multinational GNSS interference awareness initiatives [34], [35].

3.3 *GNSS-SAM in Context of Navigation Warfare (NAVWAR)*

Within the NAVWAR framework, GNSS-SAM plays a role analogous to that of a common operational picture. NAVWAR encompasses deliberate actions intended to degrade, deny, or deceive an adversary's navigation capabilities, with GNSS a primary target due to its central role in modern PNT architectures. In this context, GNSS-SAM provides commanders and operators with visibility into the navigation domain, which has traditionally been less observable than physical or cyber domains.

GNSS-SAM enables early detection of hostile NAVWAR activities by correlating anomalies across multiple receivers and platforms. For example, simultaneous loss of GNSS service across geographically separated units may indicate wide-area jamming, while coherent position deviations among

mobile assets may suggest coordinated spoofing. By presenting such information in a unified geospatial view, GNSS-SAM supports rapid threat assessment and response coordination.

Beyond detection, GNSS-SAM contributes to operational resilience by informing mitigation strategies. Knowledge of interference boundaries and severity allows operators to reroute platforms, adjust mission planning, or activate alternative navigation and timing sources. In military environments, GNSS-SAM outputs may also be fused with intelligence, surveillance, and reconnaissance (ISR) data to support attribution and targeting of interference sources.

Finally, the integration of GNSS-SAM into command-and-control systems reflects a broader shift toward treating PNT as a contested and managed resource rather than an assured utility. As NAVWAR capabilities continue to evolve, GNSS-SAM architectures are expected to play an increasingly important role in maintaining operational effectiveness across all domains, a trend clearly aligned with the motivations outlined in the accompanying presentation [5], [6], [7].

4 OBJECTIVES AND FUNCTIONAL REQUIREMENTS OF GNSS-SAM

4.1 *Real-Time GNSS Performance Monitoring*

A fundamental objective of GNSS-SAM is the continuous, near real-time monitoring of GNSS signal performance across a geographically distributed set of sensors. Unlike post-processed quality assessment, real-time monitoring enables immediate awareness of abnormal conditions that may indicate interference, system misconfiguration, or environmental disturbances. This requirement is particularly critical in safety-of-life and mission-critical applications, where delayed awareness may translate directly into operational risk.

Real-time monitoring within GNSS-SAM typically relies on the collection of low-level signals and navigation observables, such as C/N_0, satellite tracking status, pseudo-range residuals, and receiver position or timing consistency. As highlighted in the presentation, sudden, correlated deviations in these metrics, especially when observed across multiple sensors, serve as early indicators of GNSS service degradation. The system must therefore support high-rate data ingestion and low-latency processing pipelines.

Another important functional requirement is temporal coherence. GNSS-SAM must ensure precise time alignment of measurements originating from heterogeneous sensors, often operating under different clocks and network conditions. Accurate timestamping, buffering, and synchronization are prerequisites for meaningful cross-sensor correlation, particularly when detecting fast-evolving interference phenomena such as pulsed jamming or transient spoofing attempts [4].

Finally, scalability is essential for real-time monitoring. GNSS-SAM architectures should be capable of handling anything from a small regional sensor network to thousands of distributed receivers without compromising responsiveness. This requirement strongly influences system design choices for data transport, processing architectures, and cloud- or edge-based deployment models [13].

4.2 *Interference Detection and Classification*

Beyond raw monitoring, GNSS-SAM is required to detect and classify interference events in an automated and reliable manner. Detection refers to identifying deviations from nominal GNSS behavior, while classification aims to determine the nature of the underlying cause, such as jamming, spoofing, or benign environmental effects. These functions form the analytical core of GNSS-SAM systems.

Detection mechanisms are typically based on thresholding, statistical change detection, or pattern recognition applied to signal-level indicators. For example, abrupt and broadband C/N_0 degradation across multiple frequencies may indicate jamming, whereas subtle distortions in correlation functions or inconsistencies in satellite geometry may point toward spoofing [23]. The presentation emphasizes that no single indicator is sufficient, reinforcing the need for multi-feature analysis.

Classification requires the fusion of multiple indicators over time and space. Rule-based approaches remain attractive due to their transparency and ease of validation, particularly in regulated environments. However, as interference scenarios become more complex, machine learning (ML) techniques (trained on labeled interference data) are increasingly explored to enhance discrimination performance [36], [37], [38]. GNSS-SAM should support both approaches, allowing gradual evolution of detection logic.

An important functional requirement is robustness against false alarms. Excessive false positives can undermine operator trust and reduce the operational value of GNSS-SAM. Therefore, detection and classification modules must incorporate confidence measures and contextual information, such as known maintenance events or ionospheric activity, to reduce ambiguity [5].

4.3 *Alerting and Notification Mechanisms*

A key operational objective of GNSS-SAM is to translate detected interference events into timely and actionable alerts. Alerting mechanisms serve as the primary interface between the situational awareness system and its users, enabling rapid response to emerging GNSS threats. Effective alerting requires careful balancing between responsiveness and information overload.

Alerts in GNSS-SAM are typically generated when predefined thresholds or confidence levels are exceeded. As illustrated in the presentation, examples include sudden C/N_0 drops greater than a specified value, simultaneous anomalies reported by multiple receivers, or detection of spoofing indicators persisting beyond a defined duration. These triggers must be configurable to accommodate different operational contexts, such as aviation, maritime, or telecommunications environments.

Notification mechanisms should support multiple delivery channels, including visual indicators on the GNSS-SAM interface, automated messages (e.g., email or network notifications), and machine-to-machine (M2M) interfaces for integration with external systems. In critical infrastructures, alerts may directly trigger fallback procedures, such as switching to alternative timing sources or non-GNSS navigation modes.

Equally important is the content of alerts. GNSS-SAM alerts should convey not only the existence of a problem, but also its estimated severity, spatial extent, and confidence level. This enables operators to prioritize responses and avoid unnecessary operational disruptions [34], [35].

4.4 *Historical Data Analysis and Forensic Capabilities*

In addition to real-time functions, GNSS-SAM must support historical data storage and post-event analysis. Archiving past measurements and detected events enables forensic investigations, trend analysis, and system performance evaluation. This capability is particularly valuable for understanding recurring interference patterns and assessing long-term GNSS resilience.

Historical analysis allows operators to correlate GNSS interference events with external factors such as geographic location, time of day, or known activities. For example, repeated jamming incidents near specific infrastructure or borders may indicate persistent interference sources. GNSS-SAM systems should therefore support efficient querying, visualization, and replay of historical data [39].

From a system development perspective, archived data also serve as an essential resource for improving detection and classification algorithms. Labeled historical events can be used to refine thresholds, validate rule-based logic, or train ML models. This feedback loop supports continuous improvement of GNSS-SAM performance over time.

Finally, forensic capabilities contribute to accountability and reporting. In regulated domains such as aviation or critical infrastructure protection, documented evidence of GNSS interference may be required for incident reporting, regulatory compliance, or coordination with national authorities. GNSS-SAM thus functions not only as a real-time awareness tool, but also as a long-term knowledge repository [40].

5 GNSS-SAM DATA SOURCES AND SENSOR NETWORKS

5.1 *Fixed GNSS Reference Stations*

Permanent GNSS reference stations constitute one of the most reliable and widely used data sources for GNSS-SAM systems. These stations operate at known, precisely surveyed locations and provide continuous observations of GNSS signals with high temporal stability. Their fixed geometry and long-term operation make them particularly suitable for detecting persistent or wide-area interference affecting GNSS service quality.

GNSS-SAM systems can leverage data from existing national and international reference networks, including CORSs, the International GNSS Service (IGS), and satellite-based augmentation system (SBAS) monitoring infrastructures [41], [42], [43], [44]. Although originally designed for precise positioning, geodesy, or integrity monitoring, these networks deliver rich signal-level observables that can be repurposed for interference detection and situational awareness.

A key limitation of fixed-reference networks is their spatial distribution, which is often driven by geodetic or aviation requirements rather than by interference-monitoring needs. As a result, sensor density may be uneven, with sparse coverage in remote or maritime areas. GNSS-SAM architectures must therefore account for heterogeneous sensor spacing and employ spatial correlation or interpolation techniques when visualizing service degradation [42], [45].

Despite these limitations, permanent reference stations remain a cornerstone of GNSS-SAM due to their high data quality, operational stability, and availability of real-time data streams through standardized protocols such as NTRIP (i.e., Networked Transport of RTCM via Internet Protocol, where RTCM means the Radio Technical Commission for Maritime Services), enabling near real-time situational awareness [46], [47], [48].

5.2 *Mobile Platforms and Opportunistic Sensors*

Mobile sensing platforms provide an important complement to fixed GNSS reference stations in GNSS-SAM systems. These platforms include land vehicles, maritime vessels, aircraft, and unmanned aerial vehicles (UAVs), which are capable of collecting GNSS measurements while traversing areas that are insufficiently covered by permanent infrastructure. Mobile sensors enable dynamic exploration of interference-affected regions and support spatial characterization of GNSS disruptions.

In the GNSS-SAM context, mobile platforms are particularly valuable for mapping the spatial extent of interference and for assisting in source localization. As the platform moves through different environments, variations in signal quality can be observed as a function of position, providing information that is not available from stationary sensors. As highlighted in the presentation, such data can be visualized as trajectories or velocity vectors overlaid on the situational awareness map.

However, GNSS data collected from mobile platforms are inherently more variable than data from fixed stations. Motion-induced dynamics, changing satellite visibility, multipath effects, and signal blockage can introduce fluctuations that are unrelated to interference. GNSS-SAM systems must therefore incorporate filtering, normalization, and context-aware processing to distinguish genuine interference signatures from mobility-related effects.

In addition to dedicated mobile platforms, opportunistic sensors embedded in consumer devices, such as smartphones, represent a growing data source for GNSS-SAM. Although individual measurements are less precise, the large number of available devices

can provide valuable coarse-grained insight into GNSS performance, particularly in densely populated urban environments [10].

Such opportunistic sensing approaches enable large-scale, low-cost monitoring, albeit with lower measurement reliability and increased uncertainty.

5.3 *Specialized Interference Monitoring Sensors*

Specialized interference monitoring sensors form the most advanced data layer within GNSS-SAM architectures. These sensors are specifically designed to analyze GNSS signals at a detailed level, often employing SDR technology to provide access to raw signal samples in the time and frequency domains. Such capabilities enable precise characterization of interference waveforms and spectral signatures.

These sensors can detect a wide range of interference types, including continuous-wave signals, pulsed jamming, broadband noise, and spoofing-related distortions of the correlation function. When combined with multi-antenna configurations, such as controlled reception pattern antennas (CRPAs), they can also support direction-of-arrival estimation, which is valuable for identifying and localizing interference sources [49], [50].

Within GNSS-SAM, data from specialized sensors often serve as a high-confidence reference for validating events detected by less capable receivers. Their inclusion significantly improves classification reliability, particularly in complex spoofing scenarios where subtle signal anomalies must be distinguished from benign effects.

Due to their cost and operational complexity, these sensors are typically deployed at critical locations, such as airports, seaports, telecommunications hubs, or military facilities. Integrating their outputs into a GNSS-SAM framework allows localized high-fidelity measurements to contribute to a broader, area-wide situational awareness picture [5].

5.4 *Data Integration, Synchronization, and System Architecture*

A central challenge in GNSS-SAM systems is the integration of data originating from heterogeneous sensors with differing accuracy, update rates, and reliability. The system must support both continuous real-time data streams and asynchronously reported measurements, while maintaining a coherent analytical framework. Effective data integration is therefore a core functional requirement of GNSS-SAM.

Accurate time synchronization is particularly critical. Misaligned timestamps can lead to incorrect spatial or temporal correlations, masking genuine interference events or generating false alarms. GNSS-SAM architectures typically employ normalization, buffering, and quality control mechanisms to ensure temporal consistency across data sources.

From a network perspective, GNSS-SAM can be implemented using centralized, distributed, or hybrid architectures. Increasingly, edge computing approaches are employed to perform preliminary processing near the data source, reducing communication latency and bandwidth requirements. This is especially relevant for mobile or bandwidth-constrained platforms.

A flexible and modular integration architecture enables GNSS-SAM systems to evolve over time, accommodating new sensor types, data formats, and analytical methods. Such adaptability is essential in the face of rapidly evolving GNSS interference threats and monitoring technologies [39], [40], [51]. The overall conceptual architecture of the proposed GNSS-SAM framework, including heterogeneous sensor integration, feature extraction, interference detection, and operational awareness components, is depicted in Figure 1.

The integrated and synchronized data streams form the basis for subsequent feature extraction and interference detection processes described in Section 6. Overall, GNSS-SAM data sources and sensor networks provide a multi-layered observation framework that enables robust, scalable, and context-aware situational awareness of GNSS performance.

6 SIGNAL FEATURES AND INTERFERENCE INDICATORS

6.1 *Signal-Level Metrics*

Signal-level metrics constitute the primary layer of information used in GNSS-SAM systems to assess the quality and integrity of received signals. Among these, the C/N_0 is one of the most widely used indicators, as it directly reflects the strength of the received signal relative to the noise floor. Sudden drops in C/N_0 across multiple satellites or frequencies often indicate the presence of jamming or other forms of interference [17], [18], [52].

In addition to signal strength, Doppler frequency shift (DFS) measurements provide insight into the relative motion between satellites and the receiver. Under nominal conditions, DFSs follow predictable patterns based on satellite orbits. Deviations from these expected trends, particularly when observed simultaneously across multiple satellites, may indicate spoofing attempts or receiver tracking anomalies [18], [53], [54].

Pseudo-range residuals, defined as the difference between measured and predicted pseudo-ranges, are another important indicator. Elevated residuals may arise from multipath effects, atmospheric disturbances, or interference. However, spatially correlated residual anomalies across multiple receivers are more likely to indicate deliberate interference. The combined analysis of these metrics enables robust detection of both gradual degradations and abrupt disruptions. In addition, the position dilution of precision (PDOP) can be used as a geometry-related quality indicator, since interference-induced loss of satellite tracking may degrade satellite geometry and increase the expected uncertainty of the positioning solution [55], [56].

Signal quality monitoring (SQM) techniques provide an additional layer of signal-level analysis by evaluating distortions in the correlation function and tracking behavior of GNSS signals. Originally developed for safety-critical applications such as

satellite-based augmentation systems (SBASs) and ground-based augmentation systems (GBASs), SQM methods rely on metrics derived from the shape and symmetry of the correlation function, including early-minus-late measurements and slope asymmetry indicators. These metrics enable the detection of subtle signal anomalies that may not be observable through conventional indicators such as C/N_0 or pseudo-range residuals. In the context of GNSS-SAM, SQM features enhance the capability to identify spoofing and other signal deformations at an early stage, particularly when combined with spatial and multi-receiver analysis [57], [58], [59].

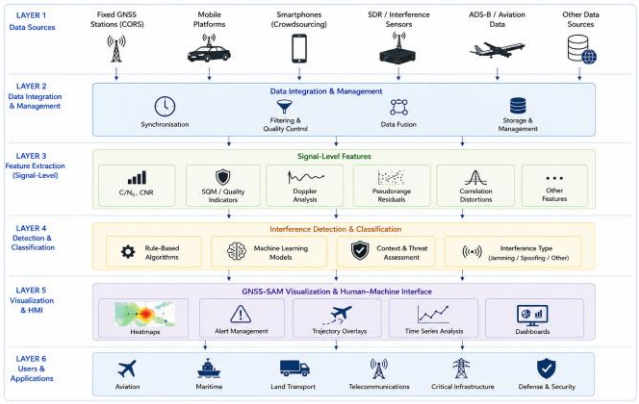


Figure 1. Conceptual architecture of the GNSS-SAM framework integrating heterogeneous sensor networks, feature extraction mechanisms, interference detection modules, geospatial visualization, and operational awareness services.

6.2 *Correlation Function Distortions*

The correlation function represents the fundamental mechanism by which GNSS receivers acquire and track satellite signals. Under nominal conditions, the correlation peak exhibits a well-defined symmetric shape. However, the presence of interference, particularly spoofing, can introduce distortions that alter this shape in detectable ways [60].

Spoofing signals, especially those generated by sophisticated transmitters, may produce multiple correlation peaks or asymmetric distortions in the correlation function. These anomalies arise from the superposition of authentic and counterfeit signals or from mismatches in code phase alignment. Monitoring such distortions provides a powerful means of detecting spoofing without relying solely on navigation-domain inconsistencies. Representative examples of signal degradation effects and interference-related indicators commonly used in GNSS-SAM systems are presented in Figure 2.

In GNSS-SAM systems, correlation-based indicators are often extracted from advanced receivers or SDR-based sensors capable of accessing raw signal samples. While this limits their availability in large-scale deployments, their diagnostic value is significant, particularly for validating suspected spoofing events detected using higher-level metrics [60], [61], [62].

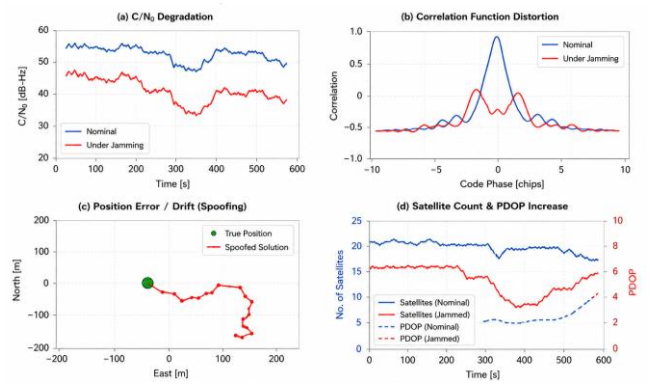


Figure 2. Examples of GNSS interference indicators used in GNSS-SAM systems, including C/N_0 degradation, correlation function distortion, spoofing-induced position drift, and satellite visibility reduction.

6.3 *Spoofing Detection Indicators*

Spoofing detection in GNSS-SAM relies on a combination of signal-level and navigation-domain indicators that reveal inconsistencies not expected under normal operating conditions. One important class of indicators is related to satellite geometry. For example, discrepancies between expected and observed satellite elevation or azimuth angles may suggest that the received signals do not originate from genuine satellite positions.

Another important indicator is the presence of time inconsistencies, such as sudden clock jumps or gradual time drift affecting multiple satellites simultaneously. Since GNSS receivers rely on precise timing for position computation, even small inconsistencies can be indicative of spoofing attempts. Monitoring these effects across multiple receivers enhances detection robustness.

Spatial correlation plays a crucial role in spoofing detection within GNSS-SAM. If multiple receivers within a region report similar position shifts or timing anomalies, this strongly suggests the presence of a coordinated spoofing attack. Conversely, isolated anomalies are more likely to be caused by local effects such as multipath.

Additional indicators include signal consistency across frequencies and constellations. Spoofing attacks often target specific signals, resulting in inconsistencies between different GNSS systems. Multi-constellation monitoring therefore, significantly improves detection capability [5], [63].

6.4 *Feature Extraction for Classification*

Feature extraction is the process of transforming raw GNSS measurements into a structured set of indicators suitable for classification and decision-making. In GNSS-SAM, this involves combining multiple signal-level metrics, correlation-based indicators, and spatial-temporal patterns into feature vectors that describe the state of the GNSS environment.

A key requirement for feature extraction is robustness against noise and environmental variability. Features must be designed to minimize sensitivity to benign effects such as multipath or atmospheric disturbances while remaining responsive

to interference signatures. This often involves normalization, filtering, and statistical aggregation over time and across sensors.

Another important aspect is dimensionality management. While a large number of features may improve detection performance, it also increases computational complexity and the risk of overfitting in ML models. GNSS-SAM systems must therefore balance feature richness with computational efficiency, particularly in real-time applications.

Finally, feature extraction serves as the interface between the data acquisition layer (see Section 5) and the analytical layer (see Section 7). Well-designed features enable effective application of both rule-based and ML approaches, forming the foundation for reliable interference detection and classification [64], [65]. The general processing workflow employed in GNSS-SAM systems for signal processing, anomaly detection, interference classification, and alert generation is illustrated in Figure 3.

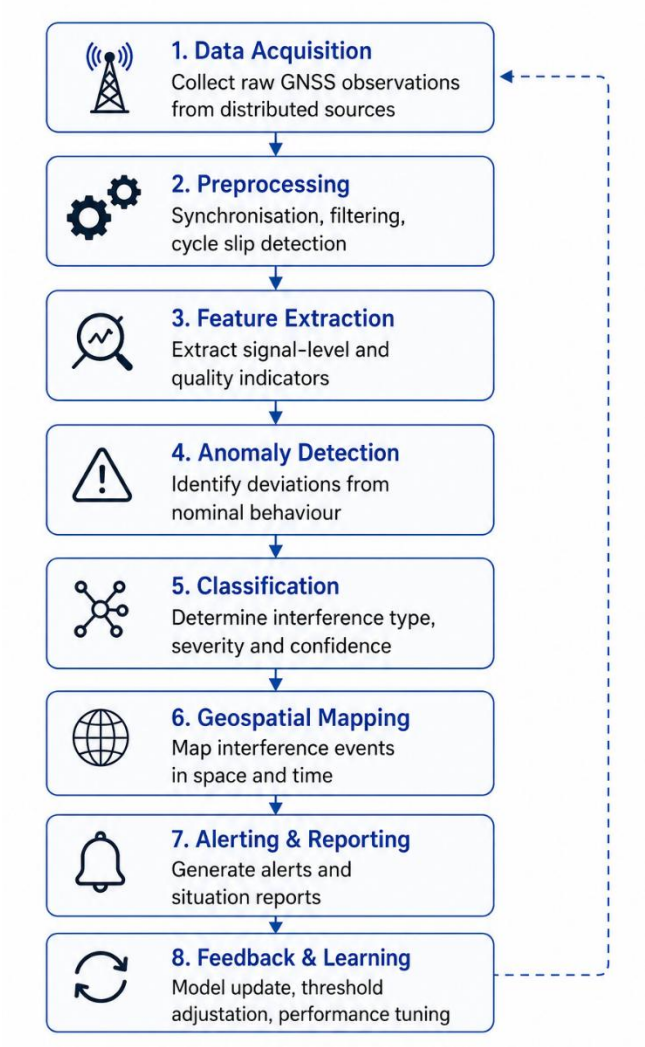


Figure 3. General workflow of GNSS-SAM data processing, including signal acquisition, preprocessing, feature extraction, anomaly detection, classification, geospatial mapping, and alert generation.

7 DATA FUSION AND ANOMALY CLASSIFICATION IN GNSS-SAM

7.1 *Rule-Based Detection Approaches*

Rule-based detection remains one of the most widely used approaches in GNSS interference monitoring systems due to its simplicity, transparency, and ease of validation. These methods rely on predefined thresholds and logical conditions applied to signal features, such as C/N_0 drops, residual thresholds, or consistency checks across receivers.

One advantage of rule-based systems is their interpretability. Each detection decision can be traced back to specific conditions, which is particularly important in safety-critical applications such as aviation. This transparency facilitates certification and regulatory acceptance, where explainability is a key requirement.

However, rule-based approaches have limitations in handling complex or evolving interference scenarios. Fixed thresholds may not generalize well across different environments, leading to false alarms or missed detections. GNSS-SAM systems often address this by incorporating adaptive thresholds or combining multiple rules to improve robustness [66], [67].

7.2 *Machine Learning-Based Classification*

ML approaches offer a more flexible framework for GNSS interference classification by learning patterns directly from data. Supervised learning techniques, such as support vector machines, random forests, or neural networks, can be trained to distinguish between nominal conditions and different types of interference based on labeled datasets.

These methods are particularly effective in detecting subtle or previously unseen interference patterns that may not be captured by rule-based systems. By leveraging large datasets collected from GNSS-SAM networks, ML models can improve detection accuracy and reduce false alarm rates.

Nevertheless, the application of ML in GNSS-SAM introduces challenges related to training data availability, model interpretability, and computational requirements. Ensuring that models generalize across different environments and remain robust to changing conditions is a key research challenge [66], [68], [69], [70].

7.3 *Event Characterization and Severity Assessment*

Once an interference event has been detected and classified, GNSS-SAM systems must characterize its properties to support decision-making. This includes identifying the type of interference (e.g., jamming, spoofing), estimating its geographic extent, and determining the affected GNSS signals or constellations.

A key aspect of event characterization is geolocation. By correlating observations from multiple sensors, GNSS-SAM can estimate the location of the interference source or define a bounding region where signal degradation is observed. The accuracy of this

process depends on sensor density and measurement quality.

Severity assessment is typically performed using a scoring system that quantifies the impact of the interference on GNSS performance. Metrics such as signal loss, position error, and affected area can be combined into a severity index, enabling prioritization of response actions.

Finally, characterized events can be visualized and communicated through GNSS-SAM interfaces, supporting both real-time operational decisions and long-term analysis. This closes the loop between data acquisition, analysis, and actionable situational awareness [34], [35], [71].

8 GEOSPATIAL VISUALIZATION AND GNSS SAM ARCHITECTURE

8.1 *GIS-Based Visualization Framework*

Geospatial visualization constitutes a central component of GNSS-SAM systems, enabling the transformation of distributed GNSS measurements into an intuitive operational picture. GIS frameworks provide the underlying infrastructure for integrating spatial data layers, including base maps, infrastructure elements, and GNSS performance indicators. By leveraging GIS technologies, GNSS-SAM systems can present heterogeneous data in a unified and georeferenced form.

A typical GIS-based GNSS-SAM architecture consists of multiple layers, including a base map (e.g., OpenStreetMap [72] or satellite imagery), sensor locations, and dynamically updated performance metrics. These layers are continuously refreshed using real-time data streams and are often combined with temporal filtering mechanisms to provide a near real-time view of GNSS conditions. The use of standardized spatial data formats and web-based GIS services facilitates interoperability and scalability.

Furthermore, GIS frameworks support advanced spatial analysis functions, such as interpolation, clustering, and spatial correlation. These capabilities are particularly important in GNSS-SAM systems, where sensor density may vary significantly across regions. Through spatial modeling techniques, it is possible to estimate GNSS performance in areas lacking direct measurements, thereby improving the completeness of situational awareness [73].

8.2 *Performance Heatmaps and Interference Markers*

Performance heatmaps are one of the most effective visualization tools used in GNSS-SAM systems. They provide a continuous spatial representation of GNSS signal quality, typically derived from aggregated metrics such as C/N_0 or positioning error. By mapping these values onto a grid and applying color-coded scales, heatmaps allow operators to quickly identify regions of degraded performance.

As described in the presentation, heatmaps often employ threshold-based color schemes, where green indicates nominal operation, yellow represents moderate degradation, and red highlights severe interference or signal denial. Such visual encoding enables rapid interpretation even under time-critical conditions. Temporal averaging (e.g., over several minutes) is commonly applied to reduce noise and highlight persistent patterns.

In addition to continuous heatmaps, discrete interference markers are used to represent detected events. These markers are typically categorized by type (e.g., continuous-wave jamming, broadband interference, spoofing) and displayed using distinct symbols or colors. When combined with temporal information, they provide a clear picture of ongoing and past interference activity.

The combination of heatmaps and event markers enhances situational awareness by providing both a global overview and localized detail. This dual representation is particularly useful in operational environments such as aviation and maritime navigation, where both regional trends and specific events must be monitored simultaneously [35], [71].

8.3 *Velocity and Trajectory Overlays*

In addition to static sensor data, GNSS-SAM systems can incorporate dynamic information from mobile platforms. Velocity vectors and trajectory overlays provide valuable insight into the interaction between moving receivers and interference environments. By visualizing movement paths alongside signal quality metrics, operators can better understand how interference affects navigation in real-world scenarios.

Trajectory overlays are particularly useful for identifying spatial boundaries of interference zones. As a mobile platform enters or exits a degraded region, changes in signal quality can be correlated with position, enabling the estimation of interference extent. This is especially relevant for UAV-based monitoring or maritime applications, where mobility is inherent to the sensing process.

Velocity vectors further enhance this analysis by indicating direction and speed of motion. When combined with temporal data, they allow the reconstruction of interference events over time, revealing patterns such as moving jamming sources or transient disturbances. An example of trajectory-based visualization and dynamic interference evolution in a GNSS-SAM environment is presented in Figure 4. This dynamic visualization capability distinguishes GNSS-SAM from static monitoring systems.

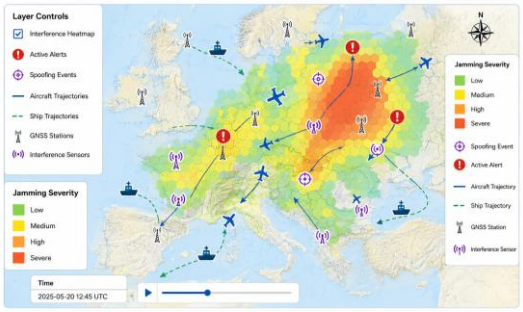


Figure 4. Example of dynamic GNSS-SAM visualization integrating trajectory overlays, mobile receiver movement, temporal interference evolution, and geospatial event correlation for operational situational awareness.

Moreover, trajectory-based analysis can support validation of detected events. Consistent degradation observed along multiple independent trajectories increases confidence in the presence of interference, while isolated anomalies may be attributed to local environmental effects [10], [74], [75].

8.4 *Human-Machine Interface for Decision Support*

The human-machine interface (HMI) plays a critical role in translating GNSS-SAM data into actionable information. Effective HMI design must balance the need for comprehensive information with the requirement for clarity and usability. This is particularly important in operational contexts where decisions must be made rapidly.

GNSS-SAM interfaces typically include multiple visualization components, such as maps, dashboards, and alert panels. Interactive features, including zooming, filtering, and time navigation, allow users to explore data at different levels of detail. Customization options enable adaptation to specific operational needs, such as aviation control or maritime monitoring.

A key requirement of HMI design is the prioritization of information. Critical alerts and severe interference events must be clearly distinguished from routine data to prevent information overload. Visual hierarchy, color coding, and alert escalation mechanisms are commonly employed to guide user attention.

Finally, GNSS-SAM interfaces should support integration with external systems, such as command-and-control platforms or network management systems. This ensures that situational awareness information can be seamlessly incorporated into broader operational workflows, enhancing overall system effectiveness [76], [77] .

9 EXISTING GNSS-SAM SOLUTIONS AND IMPLEMENTATIONS

9.1 *Public and Open GNSS Interference Monitoring Platforms*

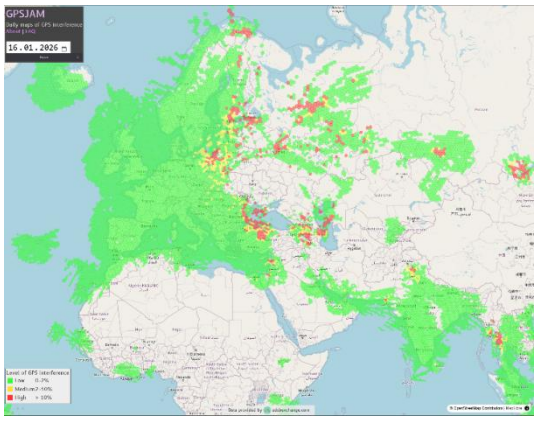
Several publicly accessible platforms provide insight into GNSS interference by aggregating data from distributed sources. These systems often rely on crowd-sourced data, aviation reports, or open sensor networks to visualize GNSS disruptions over large geographic areas. Their accessibility makes them valuable tools for both researchers and practitioners.

Such platforms include web-based services that display GNSS jamming intensity derived from aircraft navigation data or crowd-sourced measurements. They typically present heatmaps of interference levels and may incorporate temporal filtering or historical views. Although their data sources may be heterogeneous, they provide a useful approximation of GNSS conditions at a regional or global scale.

One notable advantage of these platforms is their ability to provide near real-time updates with minimal infrastructure requirements. However, their reliance on indirect measurements or non-specialized sensors may limit accuracy and reliability. Despite these limitations, they play an important role in raising awareness of GNSS interference phenomena and their operational impact [78].

Concrete examples of such platforms are illustrated in Figures 5 and 6, highlighting differences in data sources, visualization approaches, and levels of operational maturity. The GPSJam platform [78], for instance, presents global maps of GNSS interference intensity derived primarily from Automatic Dependent Surveillance–Broadcast (ADS-B) [79], [80] data collected from commercial aircraft, enabling the identification of large-scale jamming activity, as shown in Figure 5(a) [78]. Similarly, spoofing monitoring services, such as the platform developed by SkAI Data Services, present suspected spoofing events based on aviation data analytics [81].

(a)



(b)

(c)

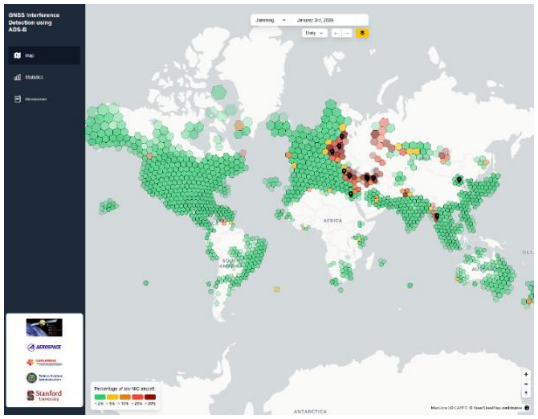


Figure 5. Examples of publicly available GNSS interference monitoring platforms: (a) GPSJam – global map of GNSS interference intensity derived primarily from ADS-B data; (b) GPSwise – real-time visualization of spoofing and jamming events with trajectory-based analytics; (c) Stanford GNSS interference monitoring platform – research-oriented system using ADS-B-derived indicators for global interference detection.

More advanced platforms, such as GPSWise, extend this approach by providing near real-time monitoring of both jamming and spoofing events, combined with trajectory-based visualization and historical analysis capabilities, thereby supporting operational awareness in aviation contexts, as illustrated in Figure 5(b) [82]. In parallel, research-oriented systems such as the Stanford GNSS interference monitoring platform (rfi.stanford.edu) employ ADS-B-derived indicators and signal quality analysis to detect and visualize interference events on a global scale, as shown in Figure 5(c) [83].

Additional insight can be obtained from commercial flight tracking services such as FlightRadar24, which infer GNSS interference from degradation of Navigation Integrity Category (NIC) values embedded in ADS-B messages. This enables the identification of regions where multiple aircraft simultaneously experience degraded positioning performance, as illustrated in Figure 6(a) [84]. A more detailed spatial representation of interference patterns can be observed in regional views of GPSJam [78] of GPSWise maps [81], [82], as shown in Figures 6(b) and 6(c), respectively, highlighting localized disruption zones.

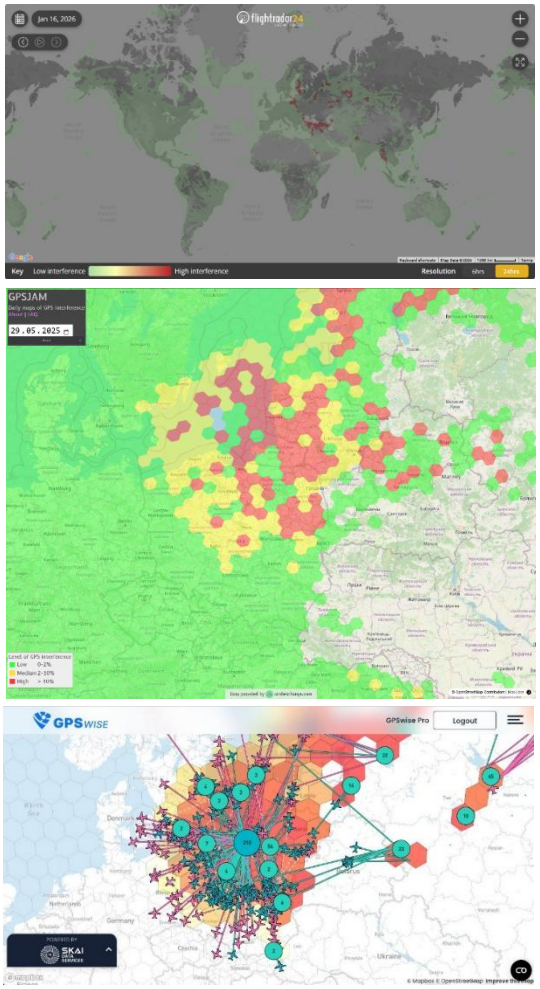


Figure 6. Additional GNSS interference visualization platforms: (a) Flightradar24 – GNSS interference inferred from degradation of Navigation Integrity Category (NIC) values in ADS-B messages; (b) GPSJam and (c) GPSwise (regional view) – detailed spatial distribution of interference levels highlighting localized disruption patterns.

At a regional level, systems such as GNSS-Finland [12] utilize data from dense CORS networks and advanced signal monitoring techniques to deliver more detailed situational awareness within specific geographic areas. Overall, these examples illustrate the diversity of current approaches, ranging from crowd-sourced and aviation-based monitoring to research-oriented and infrastructure-driven systems. A comparative overview of selected publicly available GNSS interference monitoring platforms is summarized in Table 1.

Table 1. Comparison of selected GNSS interference monitoring platforms.

Platform	Primary Data Source	Jamming Monitoring	Spoofing Monitoring	Real-Time Updates	Trajectory Overlays	Global Coverage	Data Openness
GPSJam	ADS-B (Aviation)	✓	✗	✓	✓	✓	Public
GPSwise	Aviation + Proprietary Sensors	✓	✓	✓	✓	✓	Commercial (Paid)
Stanford RFI	ADS-B + Research Algorithms	✓	✓	✓	✗	✓	Public
flightradar24	ADS-B (NIC-based)	✓	✗	✓	✓	✓	Commercial (Freemium)
GNSS-Finland	CORS + National Sensors	✓	✓	✓	✗	Regional	Public

✓ Yes ✗ No

9.2 *Commercial and Institutional GNSS-SAM Systems*

More advanced GNSS-SAM solutions are developed and operated by governmental agencies, research institutions, and commercial entities. These systems typically rely on dedicated sensor networks, including reference stations and specialized monitoring receivers, providing higher accuracy and reliability compared to open platforms.

Institutional systems, such as those developed for aviation safety, often integrate data from certified monitoring networks and apply validated detection algorithms. For example, European initiatives coordinated by European Union Aviation Safety Agency focus on monitoring GNSS interference affecting air traffic operations. Similarly, national GNSS-SA services provide continuous monitoring within specific geographic regions.

Commercial systems, on the other hand, may offer proprietary solutions tailored to specific industries, such as telecommunications or maritime operations. These systems often emphasize integration with existing infrastructure and provide advanced analytics and alerting capabilities.

Overall, institutional and commercial GNSS-SAM systems demonstrate the feasibility of large-scale, real-time monitoring. However, they are often limited by geographic scope, cost, or lack of interoperability between different systems [12].

9.3 *Limitations of Current Solutions*

Despite significant progress, existing GNSS-SAM solutions exhibit several limitations that hinder their ability to provide comprehensive situational awareness. One major challenge is the heterogeneity of data sources, which complicates integration and reduces consistency across different platforms.

Another limitation is the lack of global coverage. Many systems are confined to specific regions or rely on sparse sensor networks, leading to incomplete visibility of GNSS interference. This is particularly problematic in maritime and remote areas, where GNSS is often critical but monitoring infrastructure is limited.

Additionally, many existing platforms focus primarily on visualization rather than advanced analysis. While heatmaps and event markers provide valuable information, they may not fully capture the complexity of interference scenarios or support predictive capabilities. The integration of machine learning and advanced data fusion techniques remains an active area of research.

Finally, interoperability and standardization issues limit the ability to combine data from different systems. Addressing these challenges requires the development of unified frameworks, such as the GNSS-SAM concept proposed in this paper, which aim to integrate diverse data sources and analytical methods into a coherent and scalable solution [39].

10 USE CASES AND APPLICATIONS OF GNSS-SAM

10.1 *Aviation and Air Traffic Management*

GNSS-SAM systems play a critical role in aviation, where GNSS-based positioning is widely used for navigation, landing procedures, and air traffic management. Recent reports indicate a significant increase in GNSS jamming and spoofing incidents affecting aircraft, particularly in regions near geopolitical conflict zones, posing a direct risk to aviation safety. As a result, real-time situational awareness of GNSS performance has become essential for both pilots and air navigation service providers.

In operational contexts, GNSS-SAM can support air traffic management by providing a shared, real-time picture of interference events. Such systems enable early detection of degraded navigation performance and allow for timely mitigation actions, such as switching to alternative navigation systems or adjusting flight paths. European initiatives emphasize the importance of combining monitoring and operational data to create a unified awareness framework across aviation stakeholders .

Furthermore, GNSS-SAM contributes to post-event analysis and safety reporting. By correlating data from multiple aircraft and ground sensors, it is possible to reconstruct interference events and improve risk assessment models. This supports regulatory bodies in developing standardized procedures and mitigation strategies.

10.2 *Maritime and Port Operations*

In maritime navigation, GNSS is a fundamental component of positioning systems used by vessels, port authorities, and traffic management systems. However, GNSS signals are particularly vulnerable in coastal and high-traffic regions, where interference can disrupt vessel navigation and lead to safety risks. Recent studies have demonstrated the feasibility of detecting spoofing events using Automatic Identification System (AIS) data [85], [86], [87], highlighting the importance of large-scale monitoring approaches.

GNSS-SAM systems can enhance maritime situational awareness by integrating data from vessels, coastal stations, and satellite observations. By analyzing spatially correlated anomalies in vessel trajectories, it is possible to identify potential spoofing or jamming events affecting multiple ships simultaneously. This enables port authorities to issue warnings and implement mitigation measures.

Additionally, GNSS-SAM supports the protection of critical maritime infrastructure, such as ports and offshore installations. By providing continuous monitoring and historical analysis capabilities, these systems contribute to improved resilience of maritime operations against GNSS disruptions.

10.3 *Telecommunications and Power Grid Synchronization*

GNSS is widely used as a primary source of precise timing in telecommunications networks and power grid synchronization systems. Accurate timing is essential for maintaining network synchronization, enabling data transmission, and ensuring stable operation of power systems. Disruptions in GNSS signals can therefore have cascading effects on critical infrastructure.

GNSS-SAM systems provide a mechanism for detecting timing anomalies and identifying potential interference affecting synchronization services. By monitoring signal integrity and timing consistency across distributed sensors, it is possible to detect early signs of degradation and prevent large-scale failures.

The increasing dependence on GNSS-based timing has led to growing interest in resilient PNT solutions. GNSS-SAM can support these efforts by providing real-time awareness of timing integrity and enabling the integration of alternative timing sources, such as terrestrial networks or atomic clocks, into hybrid architectures.

10.4 *Security, Defense, and Border Protection*

GNSS interference is often associated with intentional activities, including electronic warfare, smuggling, and unauthorized use of jamming devices. As such, GNSS-SAM systems have important applications in security and defense domains.

In military contexts, GNSS-SAM can support the detection and localization of interference sources, enabling rapid response and mitigation. By combining data from multiple sensors and platforms, it is possible to identify patterns of interference and assess potential threats.

Border protection agencies can also benefit from GNSS-SAM by monitoring anomalous navigation behavior in border regions. For example, spoofing may be used to conceal vessel or vehicle movements, and its detection can support law enforcement operations.

Finally, GNSS-SAM contributes to national resilience by providing situational awareness of GNSS

threats across critical infrastructure sectors. This supports coordinated responses to large-scale interference events and enhances overall security.

11 DISCUSSION AND FUTURE DIRECTIONS

11.1 *Scalability and Interoperability*

One of the key challenges in GNSS-SAM development is scalability. As the number of sensors and data sources increases, the system must efficiently process large volumes of heterogeneous data in real time. This requires scalable architectures capable of handling distributed data streams and performing real-time analytics.

Interoperability is equally important, as GNSS-SAM systems must integrate data from diverse sources, including CORS networks, mobile sensors, and commercial platforms. The lack of standardized data formats and interfaces remains a significant barrier to integration. Addressing this challenge requires the development of common data models and protocols.

Future GNSS-SAM systems are likely to adopt cloud-based and edge computing architectures to improve scalability and reduce latency. These approaches enable distributed processing and facilitate the integration of new data sources.

11.2 *Predictive Analytics and Artificial Intelligence (AI) Driven Threat Assessment*

The increasing availability of GNSS monitoring data creates opportunities for applying advanced analytics and machine learning techniques. Predictive models can be used to identify patterns of interference and anticipate future events, enabling proactive mitigation strategies.

ML approaches can also improve classification accuracy by identifying complex patterns that are not captured by rule-based methods. However, challenges remain in terms of data quality, model generalization, and interpretability.

In the context of GNSS-SAM, artificial intelligence (AI)-driven approaches are expected to play a growing role in threat assessment and decision support. By combining historical data with real-time observations, these systems can provide predictive insights into GNSS interference trends.

11.3 *Integration with Resilient PNT Architectures*

The vulnerability of GNSS to interference has led to increased interest in resilient PNT architectures. These systems combine GNSS with alternative technologies, such as terrestrial navigation systems, inertial sensors, and communication-based positioning.

GNSS-SAM plays a key role in such architectures by providing real-time awareness of GNSS performance and enabling dynamic selection of alternative positioning sources. A conceptual integration of GNSS-SAM with resilient multi-source PNT architectures is shown in Figure 7. This enhances system resilience and reduces dependence on a single technology.

Future research should focus on developing integrated frameworks that combine GNSS-SAM with multi-sensor PNT systems. Such approaches will be essential for ensuring reliable positioning and timing in the presence of increasing interference threats.

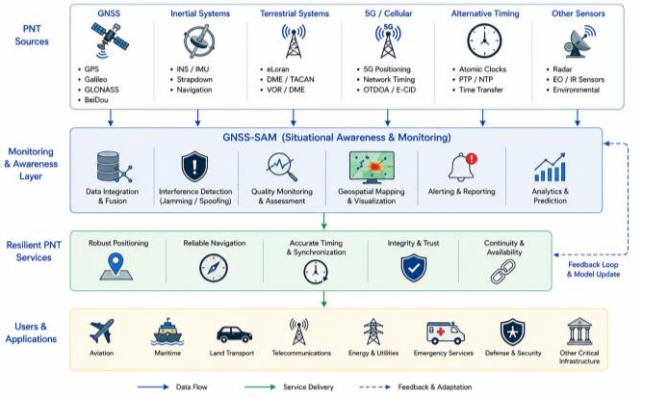


Figure 7. Integration of GNSS-SAM with resilient PNT architectures combining GNSS monitoring, alternative positioning technologies, sensor fusion, and adaptive navigation support mechanisms.

12 CONCLUSIONS

This paper has presented the concept of GNSS-SAM as a comprehensive framework for monitoring, detecting, analyzing, and visualizing GNSS interference phenomena. The proposed approach integrates heterogeneous data sources, including fixed GNSS reference stations, mobile sensing platforms, crowd-sourced observations, and specialized interference monitoring sensors, into a unified situational awareness architecture. By combining signal-level analysis, feature extraction, anomaly classification, and geospatial visualization, GNSS-SAM enables a coherent representation of GNSS performance degradation in both spatial and temporal domains.

The conducted analysis has shown that GNSS-SAM systems can significantly enhance awareness of jamming and spoofing activity across multiple operational sectors. In aviation, such systems support flight safety and air traffic management by enabling near real-time identification of navigation disruptions. In maritime environments, GNSS-SAM contributes to improved monitoring of vessel navigation and port operations, while in telecommunications and power grid infrastructures it supports the protection of time synchronization services. The presented examples further demonstrate that GNSS-SAM concepts are increasingly relevant for security, defense, and critical infrastructure resilience applications.

The paper has also highlighted the growing importance of integrating data from distributed and heterogeneous monitoring infrastructures. Existing platforms, including public, research-oriented, and commercial systems, already demonstrate the feasibility of large-scale GNSS interference monitoring using data derived from ADS-B observations, CORS networks, and signal quality indicators. However, current solutions often remain fragmented, application-specific, or geographically limited. The GNSS-SAM concept addresses these limitations by promoting a scalable and interoperable framework

capable of combining diverse sensing modalities and analytical techniques into a unified operational picture.

Particular attention has been devoted to signal-level metrics and interference indicators, including C/N_0 degradation, Doppler anomalies, pseudo-range residuals, SQM, and correlation function distortions. These features constitute the foundation for both rule-based and ML-based interference classification approaches. The analysis indicates that future GNSS-SAM systems will increasingly rely on data fusion, predictive analytics, and AI-driven threat assessment mechanisms to improve detection reliability and reduce false alarm rates.

Despite significant progress in GNSS interference monitoring technologies, several challenges remain open. Scalability, interoperability, real-time processing, and standardized data exchange mechanisms continue to represent important research and engineering issues. Furthermore, the increasing sophistication of spoofing techniques requires the development of more advanced detection algorithms and resilient monitoring architectures.

Future work should therefore focus on the integration of GNSS-SAM with resilient PNT frameworks combining GNSS, inertial systems, terrestrial positioning technologies, and alternative timing sources. The proposed GNSS-SAM framework remains conceptual and requires validation using operational multi-sensor datasets and large-scale deployments. Future GNSS-SAM architectures should also consider cyber resilience, secure data exchange mechanisms, and trustworthiness assessment of distributed monitoring networks to ensure reliable situational awareness under contested operational conditions.

Overall, GNSS-SAM represents a promising direction for the development of next-generation GNSS monitoring and resilience systems. By transforming distributed GNSS observations into actionable operational awareness, these systems can support both civilian and governmental stakeholders in mitigating the impact of intentional and unintentional GNSS interference. As dependence on satellite-based positioning, navigation, and timing services continues to increase, comprehensive situational awareness solutions such as GNSS-SAM will become an increasingly important component of resilient PNT ecosystems.

ABBREVIATIONS

ADS B – Automatic Dependent Surveillance–Broadcast
AI – artificial intelligence
AIS – Automatic Identification System
C/N_0 – carrier-to-noise density ratio
CORS – continuously operating reference station
CRPA – controlled reception pattern antenna
CW – continuous-wave
DFS – Doppler frequency shift
EW – electronic warfare
FGI – Finnish Geospatial Research Institute
GBAS – ground-based augmentation system
GIS – geographic information system
GNSS – global navigation satellite system
GNSS-SA – GNSS situational awareness
GNSS-SAM – GNSS situational awareness map
HAS – High Accuracy Service
HMI – human-machine interface
IGS – International GNSS Service
ISR – intelligence, surveillance, and reconnaissance
M2M – machine-to-machine
ML – machine learning
NAVWAR – navigation warfare
NTRIP – Networked Transport of RTCM via Internet Protocol
OSNMA – Open Service Navigation Message Authentication
PDOP – position dilution of precision
PMU – phasor measurement unit
PNT – positioning, navigation, and timing
RF – radio-frequency
RTCM – Radio Technical Commission for Maritime Services
SBAS – satellite-based augmentation system
SDR – software-defined radio
SQM – signal quality monitoring
UAV – unmanned aerial vehicle

ACKNOWLEDGEMENTS

This work was developed within the framework of the research grants no. UGB/531-000059-W300-22/2025 on "Transmission properties of radio wave propagation environments in military applications" and no. UGB/531-000128-W300-22/2026 on "Possibility analysis of using modern technologies in communication systems and electronic warfare", sponsored by the Military University of Technology (WAT), Poland.

REFERENCES

[1] E. Kaplan and C. J. Hegarty, Understanding GPS/GNSS: Principles and applications, 3rd ed. in GNSS Technology and Applications Series. Boston, MA, USA; London, UK: Artech House, 2017.
[2] L. Meng, L. Yang, W. Yang, and L. Zhang, "A survey of GNSS spoofing and anti-spoofing technology," Remote Sensing, vol. 14, no. 19, p. 4826, Jan. 2022, doi: 10.3390/rs14194826.
[3] K. Radoš, M. Brkić, and D. Begušić, "Recent advances on jamming and spoofing detection in GNSS," Sensors, vol. 24, no. 13, p. 4210, Jan. 2024, doi: 10.3390/s24134210.
[4] J. Dułowicz, P. Skokowski, and J. M. Kelner, "Survey on intentional interference techniques of GNSS signals and radio links between unmanned aerial vehicle and ground control station," TransNav, International Journal on Marine Navigation and Safety of Sea Transportation, vol. 19, no. 3, pp. 931–939, Sep. 2025, doi: 10.12716/1001.19.03.27.
[5] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," Proceedings of the IEEE, vol. 104, no. 6, pp. 1258–1270, Jun. 2016, doi: 10.1109/JPROC.2016.2526658.
[6] A. Ahmad, "Electronic warfare in NAVWAR: Impact of electronic attacks on GNSS / GBAS approach service types C and D landing systems and their proposed electronic protection measures (EPM)," Hadmérnök, vol. 14, no. 2, pp. 238–255, Jun. 2019, doi: 10.32567/hm.2019.2.20.
[7] A. Ahmad, "Navigation warfare (NAVWAR): Balancing the position in space between GPS and Galileo," Hadmérnök, vol. 14, no. 4, pp. 163–177, 2019, doi: 10.32567/hm.2019.4.10.
[8] A. A. Ragel, "GNSS-based non-cooperative air traffic situational awareness," M.Sc. thesis, Technische Universität München, Munich, Germany, 2023. Accessed: Jan. 16, 2026. [Online]. Available: https://elib.dlr.de/202083/

[9] J. Timonen and J. Vankka, "Enhancing situational awareness by means of visualization and information integration of sensor networks," in Proceedings of SPIE: Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications 2013, Baltimore, MD, USA: SPIE, Apr. 2013, pp. 250–263. doi: 10.1117/12.2017686.

[10] M. Spanghero, F. Geib, R. Panier, and P. Papadimitratos, "Uncovering GNSS interference with aerial mapping UAV," in 2024 IEEE Aerospace Conference, Big Sky, MT, USA, Mar. 2024, pp. 1–10. doi: 10.1109/AERO58975.2024.10521434.

[11] H. L. Nguyen et al., "Situational awareness: Mapping interference sources in real-time using a smartphone app," Sensors, vol. 18, no. 12, p. 4130, Nov. 2018, doi: 10.3390/s18124130.

[12] T. Hammarberg, F. S. Prol, M. Z. H. Bhuiyan, T. Hammarberg, F. S. Prol, and M. Z. H. Bhuiyan, "Enhancing GNSS situational awareness by monitoring the new Galileo services," Engineering Proceedings, vol. 88, no. 1, p. e69, Aug. 2025, doi: 10.3390/engproc2025088069.

[13] J. Zidan, E. I. Adegoke, E. Kampert, S. A. Birrell, C. R. Ford, and M. D. Higgins, "GNSS vulnerabilities and existing solutions: A review of the literature," IEEE Access, vol. 9, pp. 153960–153976, 2021, doi: 10.1109/ACCESS.2020.2973759.

[14] S. M. Sánchez-Naranjo et al., "GNSS vulnerabilities," in Multi-technology positioning, J. Nurmi, E.-S. Lohan, H. Wymeersch, G. Seco-Granados, and O. Nykänen, Eds., Cham, Switzerland: Springer International Publishing, 2017, pp. 55–77. doi: 10.1007/978-3-319-50427-8_4.

[15] D. Zmysłowski, M. Kryk, and J. M. Kelner, "Testing GNSS receiver robustness for jamming," Aviation and Security Issues, vol. 4, no. 2, Art. no. 2, Dec. 2023, doi: 10.55676/asi.v4i2.64.

[16] M. Cuntz, A. Konovaltsev, A. Dreher, and M. Meurer, "Jamming and spoofing in GPS/GNSS based applications and services – Threats and countermeasures," in Future Security, N. Aschenbruck, P. Martini, M. Meier, and J. Tölle, Eds., in Communications in Computer and Information Science. Berlin, Heidelberg, Germany: Springer, 2012, pp. 196–199. doi: 10.1007/978-3-642-33161-9_29.

[17] F. Zhou, H. Wang, Z. Zhou, Y. Xiao, and H. Li, "Carrier-to-noise ratio periodicity deviation monitoring for GNSS spoofing detection at timing and reference stations," IEEE Sensors Journal, vol. 26, no. 8, pp. 12228–12239, Apr. 2026, doi: 10.1109/JSEN.2026.3669197.

[18] X. Wei, C. Sun, X. Li, and J. Ma, "GNSS spoofing detection for UAVs using Doppler frequency and carrier-to-noise density ratio," Journal of Systems Architecture, vol. 153, p. 103212, Aug. 2024, doi: 10.1016/j.sysarc.2024.103212.

[19] J. Magiera, "A multi-antenna scheme for early detection and mitigation of intermediate GNSS spoofing," Sensors, vol. 19, no. 10, p. 2411, Jan. 2019, doi: 10.3390/s19102411.

[20] Z. Wu, Y. Zhang, Y. Yang, C. Liang, and R. Liu, "Spoofing and anti-spoofing technologies of global navigation satellite system: A survey," IEEE Access, vol. 8, pp. 165444–165496, 2020, doi: 10.1109/ACCESS.2020.3022294.

[21] E. Falletti, D. Margaria, G. Marucco, B. Motella, M. Nicola, and M. Pini, "Synchronization of critical infrastructures dependent upon GNSS: Current vulnerabilities and protection provided by new signals," IEEE Systems Journal, vol. 13, no. 3, pp. 2118–2129, Sep. 2019, doi: 10.1109/JSYST.2018.2883752.

[22] M. Filić, "Foundations of GNSS spoofing detection and mitigation with distributed GNSS SDR receiver," TransNav, International Journal on Marine Navigation and Safety od Sea Transportation, vol. 12, no. 4, pp. 649–656, Dec. 2018, doi: 10.12716/1001.12.04.01.

[23] Y. Hu, S. Bian, K. Cao, and B. Ji, "GNSS spoofing detection based on new signal quality assessment model," GPS Solutions, vol. 22, no. 1, p. 28, Jan. 2018, doi: 10.1007/s10291-017-0693-7.

[24] D. Medina, C. Lass, E. P. Marcos, R. Ziebold, P. Closas, and J. García, "On GNSS jamming threat from the maritime navigation perspective," in 2019 22th International Conference on Information Fusion (FUSION), Ottawa, ON, Canada, Jul. 2019, pp. 1–7. doi: 10.23919/FUSION43075.2019.9011348.

[25] J. Orbán, "Overview of GNSS interference risks in transport safety and resilient responses," Engineering Proceedings, vol. 113, no. 1, p. 42, Nov. 2025, doi: 10.3390/engproc2025113042.

[26] H. Nasser et al., "GNSS interference detection and geolocalization for aviation applications," in 2022 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS), Denver, CO, USA, Sep. 2022, pp. 192–216. doi: 10.33012/2022.18358.

[27] P. Zalewski, "GNSS integrity concepts for maritime users," in 2019 European Navigation Conference (ENC), Warsaw, Poland, Apr. 2019, pp. 1–10. doi: 10.1109/EURONAV.2019.8714188.

[28] T. Wührl, M. T. Baross, S. Gyányi, and P. J. Varga, "5G synchronization problems with GNSS interference," in 2023 IEEE 6th International Conference and Workshop Óbuda on Electrical and Power Engineering (CANDO-EPE), Oct. 2023, pp. 149–154. doi: 10.1109/CANDO-EPE60507.2023.10417998.

[29] S. Tang, C. Liu, W. Ding, S. Guo, and W. Yao, "Microsecond-level synchronization solution for grid-edge devices utilizing cellular networks in GNSS-challenged areas," IEEE Transactions on Industrial Informatics, vol. 21, no. 6, pp. 4713–4723, Jun. 2025, doi: 10.1109/TII.2025.3545095.

[30] L. Setlak, R. Kowalik, L. Setlak, and R. Kowalik, "Study and analysis of interference signals of the LTE system of the GNSS receiver," Sensors, vol. 21, no. 14, p. 4901, Jul. 2021, doi: 10.3390/s21144901.

[31] T. Jones et al., "Recent advances in precision clock synchronization protocols for power grid control systems," Energies, vol. 14, no. 17, p. 5303, Aug. 2021, doi: 10.3390/en14175303.

[32] A. G. Phadke and T. Bi, "Phasor measurement units, WAMS, and their applications in protection and control of power systems," Journal of Modern Power Systems and Clean Energy, vol. 6, no. 4, pp. 619–629, Jul. 2018, doi: 10.1007/s40565-018-0423-3.

[33] J. De La Ree, V. Centeno, J. S. Thorp, and A. G. Phadke, "Synchronized phasor measurement applications in power systems," IEEE Transactions on Smart Grid, vol. 1, no. 1, pp. 20–27, Jun. 2010, doi: 10.1109/TSG.2010.2044815.

[34] M. Sammueller, "GNSS threat detection & integrity monitoring. A research-based framework and operational implementation," presented at the Joint ICAO Europe and North Atlantic (EUR/NAT) and Middle East (MID) Workshop on Global Navigation Satellite System (GNSS) Radio Frequency Interference (RFI), Nov. 19, 2025.

[35] S. Thombre et al., "GNSS threat monitoring and reporting: Past, present, and a proposed future," The Journal of Navigation, vol. 71, no. 3, pp. 513–529, May 2018, doi: 10.1017/S0373463317000911.

[36] P. Gao, S. Sun, Z. Zeng, and C. Wang, "GNSS spoofing jamming recognition based on machine learning," in Signal and Information Processing, Networking and Computers. ICSINC 2017. Lecture Notes in Electrical Engineering, S. Sun, N. Chen, and T. Tian, Eds., Singapore: Springer, 2018, pp. 221–228. doi: 10.1007/978-981-10-7521-6_27.

[37] B. Pardhasaradhi, R. R. Yakkati, and L. R. Cenkeramaddi, "Machine learning-based screening and measurement to measurement association for navigation in GNSS spoofing environment," IEEE Sensors Journal, vol. 22, no. 23, pp. 23423–23435, Dec. 2022, doi: 10.1109/JSEN.2022.3214349.

[38] A. Ghanbarzade and H. Soleimani, "GNSS/GPS spoofing and jamming identification using machine learning and deep learning," Jan. 04, 2025, arXiv: arXiv:2501.02352. doi: 10.48550/arXiv.2501.02352.
[39] J. J. R. Critchley-Marrows and Q. Verspieren, "Ensuring PNT resilience in a time of navigation uncertainty," Space Policy, vol. 72, p. 101665, May 2025, doi: 10.1016/j.spacepol.2024.101665.
[40] H. Imlau, "Resilience for timing & synchronisation networks," in Strengthening Resilience and Integrity in Timing, Nov. 04, 2021. [Online]. Available: https://www.researchgate.net/publication/355916173
[41] K. Krasuski and D. Wierzbicki, "Monitoring aircraft position using EGNOS data for the SBAS APV approach to the landing procedure," Sensors, vol. 20, no. 7, p. 1945, Jan. 2020, doi: 10.3390/s20071945.
[42] "Real-Time Service (RTS)," International GNSS Service. Accessed: Jan. 18, 2026. [Online]. Available: https://igs.org/rts/
[43] M. López and V. Anton, "SBAS/EGNOS enabled devices in maritime," TransNav, International Journal on Marine Navigation and Safety of Sea Transportation, vol. 12, no. 1, pp. 23–27, Mar. 2018, doi: 10.12716/1001.12.01.01.
[44] F. van Diggelen, A-GPS: Assisted GPS, GNSS, and SBAS. in GNSS Technology and Applications Series. Boston, MA, USA: Artech House, 2009.
[45] "EGNOS | EU Agency for the Space Programme." Accessed: Jan. 18, 2026. [Online]. Available: https://www.euspa.europa.eu/eu-space-programme/egnos
[46] E. Lenz, "Networked Transport of RTCM via Internet Protocol (NTRIP) – Application and benefit in modern surveying systems," in FIG Working Week 2004, Athens, Greece, May 2004, pp. 1–11.
[47] G. Weber, D. Dettmering, and H. Gebhard, "Networked Transport of RTCM via Internet Protocol (NTRIP)," in A Window on the Future of Geodesy, F. Sansò, Ed., Berlin, Heidelberg: Springer, 2005, pp. 60–64. doi: 10.1007/3-540-27432-4_11.
[48] E. Grauberger, "What is NTRIP? RTCM Corrections for GNSS Rovers." Accessed: Jan. 18, 2026. [Online]. Available: https://rtkdata.com/what-is-ntrip-rtcm-corrections-for-gnss-rovers/
[49] J. W. Harris and D. M. Bevly, "Beam steering adaptive noise cancellation with a controlled reception pattern antenna for GNSS anti-jamming," in 2025 IEEE/ION Position, Location and Navigation Symposium (PLANS), Salt Lake City, UT, USA, Apr. 2025, pp. 337–344. doi: 10.1109/PLANS61210.2025.11028269.
[50] J. Botros, M. K. Emara, I. Goode, K. MacLeod, and J. Hautcoeur, "Phase center variation of a controlled radiation pattern antenna: Implications of null placement on positioning errors," in 2025 IEEE International Symposium on Antennas and Propagation and North American Radio Science Meeting (AP-S/CNC-USNC-URSI), Jul. 2025, pp. 1354–1357. doi: 10.1109/AP-S/CNC-USNC-URSI55537.2025.11266118.
[51] T.-P. Tseng, P.-J. Kuo, and W.-H. Tseng, "Synchronization performance assessment of GNSS-based time source in 5G communication architecture," IEEE Access, vol. 13, pp. 208055–208066, 2025, doi: 10.1109/ACCESS.2025.3641569.
[52] Ž. Bačić, D. Šugar, and Z. Nevistić, "The impact of signal interference on static GNSS measurements," Geomatics, vol. 5, no. 3, p. 39, Aug. 2025, doi: 10.3390/geomatics5030039.
[53] J. Li, X. Zhu, M. Ouyang, D. Shen, Z. Chen, and Z. Dai, "GNSS spoofing detection technology based on Doppler frequency shift difference correlation," Measurement Science and Technology, vol. 33, no. 9, p. 095109, Jun. 2022, doi: 10.1088/1361-6501/ac672a.
[54] Z. Zhou, H. Li, and M. Lu, "Doppler-based RAIM for GNSS spoofing detection in vehicular applications," IEEE Transactions on Vehicular Technology, vol. 74, no. 7, pp. 10306–10320, Jul. 2025, doi: 10.1109/TVT.2025.3543612.
[55] M. Ö. Demir, G. K. Kurt, and A. E. Pusane, "A pseudorange-based GPS spoofing detection using hyperbola equations," IEEE Transactions on Vehicular Technology, vol. 72, no. 8, pp. 10770–10783, Aug. 2023, doi: 10.1109/TVT.2023.3257228.
[56] M. Ghandchi, N. Orouji, S. Tohidi, and M. R. Mosavi, "GPS spoofing attack detection and correction in the pseudo-range of PRNs using neural network," Wireless Personal Communications, Apr. 2026, doi: 10.1007/s11277-026-12040-1.
[57] X. Jin, X. Zhang, and S. Zheng, "Indirect Kalman filtering for robust GNSS spoofing detection in signal quality monitoring," Signal Processing, vol. 239, p. 110321, Feb. 2026, doi: 10.1016/j.sigpro.2025.110321.
[58] C. Sun, J. W. Cheong, A. G. Dempster, H. Zhao, and W. Feng, "GNSS spoofing detection by means of signal quality monitoring (SQM) metric combinations," IEEE Access, vol. 6, pp. 66428–66441, 2018, doi: 10.1109/ACCESS.2018.2875948.
[59] C. Sun, J. W. Cheong, A. G. Dempster, H. Zhao, L. Bai, and W. Feng, "Robust spoofing detection for GNSS instrumentation using Q-channel signal quality monitoring metric," IEEE Transactions on Instrumentation and Measurement, vol. 70, pp. 1–15, 2021, doi: 10.1109/TIM.2021.3102753.
[60] F. Rothmaier, Y.-H. Chen, S. Lo, and T. Walter, "A framework for GNSS spoofing detection through combinations of metrics," IEEE Transactions on Aerospace and Electronic Systems, vol. 57, no. 6, pp. 3633–3647, Dec. 2021, doi: 10.1109/TAES.2021.3082673.
[61] W. Wang and Y. Hou, "GNSS induced spoofing detection based on dynamic 3-D correlation function," IEEE Transactions on Instrumentation and Measurement, vol. 73, pp. 1–18, 2024, doi: 10.1109/TIM.2024.3472768.
[62] S. Tohidi and M. R. Mosavi, "GNSS spoofing detection using a fuzzy classifier based on time–frequency analysis of the autocorrelation function," GPS Solutions, vol. 28, no. 3, p. 146, Jun. 2024, doi: 10.1007/s10291-024-01674-y.
[63] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in 2008 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS), Savannah, GA, USA, Sep. 2008, pp. 2314–2325. Accessed: May 02, 2026. [Online]. Available: http://www.ion.org/publications/abstract.cfm?jp=p&articleID=8132
[64] M. L. Psiaki, T. E. Humphreys, and B. Stauffer, "Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies," IEEE Spectrum, vol. 53, no. 8, pp. 26–53, Aug. 2016, doi: 10.1109/MSPEC.2016.7524168.
[65] J. Bhatti and T. E. Humphreys, "Hostile control of ships via false GPS signals: Demonstration and detection," NAVIGATION, vol. 64, no. 1, pp. 51–66, 2017, doi: 10.1002/navi.183.
[66] V. Ivanov, M. Scaramuzza, and R. C. Wilson, "Deep temporal semi-supervised one-class classification for GNSS radio frequency interference detection," The Journal of Navigation, vol. 77, no. 1, pp. 59–81, Jan. 2024, doi: 10.1017/S0373463324000134.
[67] S. Jeeru, L. Jiao, P.-A. Andersen, and O.-C. Granmo, "Interpretable rule-based architecture for GNSS jamming signal classification," IEEE Sensors Journal, vol. 25, no. 10, pp. 17942–17959, May 2025, doi: 10.1109/JSEN.2025.3558966.
[68] R. R. Yakkati, B. Pardhasaradhi, J. Zhou, and L. R. Cenkeramaddi, "A machine learning based GNSS signal classification," in 2022 IEEE International Symposium on Smart Electronic Systems (iSES), Warangal, India, Dec. 2022, pp. 532–535. doi: 10.1109/iSES54909.2022.00116.
[69] L. Heublein et al., "Evaluation of (un-)supervised machine learning methods for GNSS interference classification with real-world data discrepancies," Oct. 2024, pp. 1260–1293. doi: 10.33012/2024.19887.

[70] J. R. van der Merwe, D. C. Franco, T. Feigl, and A. Rügamer, "Optimal machine learning and signal processing synergies for low-resource GNSS interference classification," IEEE Transactions on Aerospace and Electronic Systems, vol. 60, no. 3, pp. 2705–2721, Jun. 2024, doi: 10.1109/TAES.2023.3349360.
[71] F. Dovis, Ed., GNSS interference threats and countermeasures. Boston, MA, USA: Artech House, 2015.
[72] "OpenStreetMap," OpenStreetMap. Accessed: Jul. 19, 2018. [Online]. Available: https://www.openstreetmap.org/
[73] P. A. Longley, M. F. Goodchild, D. J. Maguire, and D. W. Rhind, Geographic information science and systems, 4th ed. Hoboken, NJ, USA: Wiley, 2015.
[74] J. Qiao et al., "A survey of GNSS interference monitoring technologies," Frontiers in Physics, vol. 11, Mar. 2023, doi: 10.3389/fphy.2023.1133316.
[75] D. Zmysłowski, J. M. Kelner, J. Żygólski, O. Kuszpyt, and T. Woźniak, "Characterization of GNSS interference and its impact on air transport: Poland case study," in 2026 34th URSI General Assembly and Scientific Symposium (URSI GASS), Krakow, Poland, Aug. 2026, pp. 1–4.
[76] Y. Dang et al., "Situation awareness measurement model based on information categorization and cognitive process characterization for human-machine interface design," Displays, vol. 93, p. 103402, Jul. 2026, doi: 10.1016/j.displa.2026.103402.
[77] M. R. Endsley, "Design and evaluation for situation awareness enhancement," Proceedings of the Human Factors Society Annual Meeting, vol. 32, no. 2, pp. 97–101, Oct. 1988, doi: 10.1177/154193128803200221.
[78] J. Wiseman, "GPSJam – Global GNSS interference monitoring map." Accessed: Jan. 17, 2026. [Online]. Available: https://gpsjam.org/
[79] S. D. Ilcev, "Alternative maritime radio solutions for enhanced GMDSS network," TransNav Int. J. Mar. Navig. Saf. Sea Transp., vol. 16, no. 2, pp. 259–265, Jun. 2022, doi: 10.12716/1001.16.02.08.
[80] H. A. Khan, H. Khan, S. Ghafoor, and M. A. Khan, "A survey on security of Automatic Dependent Surveillance-Broadcast (ADS-B) protocol: Challenges, potential solutions, and future directions," IEEE Communications Surveys & Tutorials, vol. 27, no. 5, pp. 3199–3226, Oct. 2025, doi: 10.1109/COMST.2024.3513213.
[81] "SkAI Data Services," SkAI Data Services. Accessed: May 03, 2026. [Online]. Available: https://www.skai-data-services.com
[82] "GPSwise – Real-time GPS Spoofing & Jamming Detection," SkAI Data Services. Accessed: May 03, 2026. [Online]. Available: https://gpswise.aero/
[83] "Stanford GNSS Interference Map." Accessed: Jan. 17, 2026. [Online]. Available: https://rfi.stanford.edu/?date=2026-01-03&mode=jamming&granularity=daily&heatmap=true
[84] FlightRadar24, "Live Flight Tracker - Real-Time Flight Tracker Map," FlightRadar24. Accessed: Jan. 17, 2026. [Online]. Available: https://www.flightradar24.com/data/gps-jamming
[85] W. Drozd, M. Dziewicki, M. Waraksa, and Ł. Bibik, "Operational status of Polish AIS network," TransNav Int. J. Mar. Navig. Saf. Sea Transp., vol. 1, no. 3, pp. 251–253, Sep. 2007.
[86] Q. Hu, Y. Jiang, J. Zhang, X. Sun, and S. Zhang, "Development of an Automatic Identification System autonomous positioning system," Sensors, vol. 15, no. 11, pp. 28574–28591, Nov. 2015, doi: 10.3390/s151128574.
[87] A. Felski and K. Jaskólski, "The integrity of information received by means of AIS during anti-collision manoeuvring," TransNav Int. J. Mar. Navig. Saf. Sea Transp., vol. 7, no. 1, pp. 95–100, Mar. 2013, doi: 10.12716/1001.07.01.12.