GNSS Jamming and Spoofing Threats in UAV Navigation: Countermeasure Status and Challenges

Yejia Zeng, Zukun Lu, Xiaoyu Zhao, Zhu Xiao, *Senior Member, IEEE*, Shaojie Ni, Zhu Han, *Fellow, IEEE*, and Keqin Li, *Fellow, IEEE*

***Abstract*—Uncrewed aerial vehicles (UAVs) have become indispensable in both civilian and military applications. However, their reliance on Global Navigation Satellite System (GNSS)-based navigation exposes them to escalating threats from sophisticated jamming and spoofing attacks. These threats severely compromise operational safety and mission integrity, necessitating the development of effective countermeasures. This survey provides a comprehensive overview of GNSS interference threats specific to UAV navigation, with a focus on the analysis of jamming and spoofing attacks, and summarizes state-of-the-art techniques for interference detection and mitigation. We first review the principles of satellite navigation for UAVs and identify the inherent vulnerability of GNSS signals to interference. Then, we systematically examine existing countermeasures, including signal processing-based, array antenna-based, and artificial intelligence-based approaches, highlighting their effectiveness against jamming and spoofing. Despite these advances, significant challenges remain in ensuring robust UAV navigation in adversarial electromagnetic environments, particularly those arising from resource constraints, limited algorithmic flexibility, and the lack of UAV-specific countermeasures. To address these issues, we propose a hierarchical framework that integrates robust signal reception, intelligent algorithm optimization, and system-level collaboration. This framework provides practical strategies for enhancing the resilience of next-generation UAV navigation systems to complex interference.**

Received 19 September 2025; revised 24 February 2026; accepted 25 March 2026. Date of publication 3 April 2026; date of current version 22 April 2026. This work was supported in part by the Science and Technology Innovation Program of Hunan Province under Grant 2025RC3233 and in part by the National Natural Science Foundation of China under Grant U24A20247 and Grant 62303475. The work of Zhu Han was supported in part by U.S. National Science Foundation (NSF) under Grant ECCS-2302469 and in part by Japan Science and Technology Agency (JST) Adopting Sustainable Partnerships for Innovative Research Ecosystem (ASPIRE) under Grant JPMJAP2326. *(Corresponding author: Zukun Lu.)*

Yejia Zeng and Xiaoyu Zhao are with the College of Electronic Science and Technology, National University of Defense Technology, Changsha 410073, China, and also with the National Key Laboratory for Positioning, Navigation and Timing Technology, Changsha 410073, China (e-mail: zengyejia_7@nudt.edu.cn; zhaoxiaoyu588@126.com).

Zukun Lu and Shaojie Ni are with the College of Electronic Science and Technology, National University of Defense Technology, Changsha 410073, China (e-mail: luzukun@nudt.edu.cn; nishaojie@nudt.edu.cn).

Zhu Xiao is with the College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China (e-mail: zhxiao@hnu.edu.cn).

Zhu Han is with the Department of Electrical and Computer Engineering at the University of Houston, Houston, TX 77004 USA (e-mail: hanzhu22@gmail.com).

Keqin Li is with the Department of Computer Science, State University of New York at New Paltz, New Paltz, NY 12561 USA (e-mail: lik@newpaltz.edu).

Digital Object Identifier 10.1109/COMST.2026.3680438

***Index Terms*—Uncrewed aerial vehicles (UAV), global navigation satellite system (GNSS), jamming, spoofing, interference detection, interference mitigation.**

I. Introduction

UNCREWED aerial vehicles (UAVs) have experienced rapid growth in both market scale and application diversity, contributing to the emergence of the low-altitude economy. In July 2024, the global UAV industry increased in size by 4.7%, driven by the establishment of more than 33,000 companies and the filing of more than 29,000 UAV-related patents worldwide [1]. Recent advancements in sensor technologies and machine learning algorithms have further enhanced the environmental perception and autonomous decision-making capabilities of UAVs [2]. As a result, the global UAV market is projected to reach USD 25.9 billion by 2030 [3].

Among the various types of UAVs, medium-sized industrial-grade UAVs stand out because of their strong environmental adaptability, high reliability, and favorable cost effectiveness. Their ability to support diverse mission payloads further enables the execution of a wide range of operational tasks [4]. These advantages position such UAVs at the core of the growing low-altitude economy and tactical operations. In civilian applications, they are widely used for precision agriculture, power inspection, and disaster management [5]. The use of UAVs in these applications reduces labor requirements while improving operational safety. Owing to their flexibility and cost efficiency, these UAVs are also extensively employed in military roles, including reconnaissance, target tracking, and precision strikes [6]. Moreover, UAV swarms with distributed sensing and network communication have further expanded the scope of UAV applications (e.g., collaborative search and rescue missions) [7]. Equipped on these UAVs, multiple navigation sensors (e.g., Global Navigation Satellite System (GNSS) and Inertial Navigation System (INS) sensors) not only provide essential state information (e.g., position and velocity) to the flight control system but also obtain precise calibration data for mission payloads to ensure the reliable execution of these tasks.

As the primary source of navigation data, the GNSS provides real-time positioning, navigation, and timing (PNT) services. Advances such as modern GNSS constellations and real-time kinematic (RTK) methods have significantly

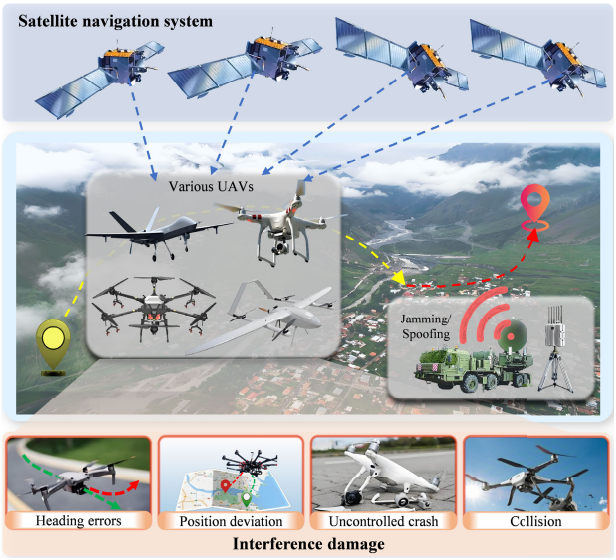


Fig. 1. GNSS interference-induced catastrophic failures in UAV navigation. Various UAVs rely on satellite navigation systems for precise navigation and positioning. However, intentional interference, particularly jamming and spoofing, compromises navigation functionality. These anomalies pose severe safety hazards.

improved the accuracy and availability of data, which has promoted high-precision, wide-area, and all-weather navigation for UAVs [8]. Empirical evidence has shown that RTK-enhanced systems (e.g., those deployed on the DJI Matrice series) significantly improve the accuracy of aerial photography by improving attitude estimation [9]. Moreover, the GNSS plays a vital role in multisensor fusion frameworks, as it corrects inertial navigation drift and enhances the robustness of visual-odometry systems [10]. This integration highlights the critical importance of the GNSS in modern UAV systems.

However, the inherent vulnerability of GNSS signals to interference poses a significant threat to the operational integrity of UAVs, directly compromising flight safety and mission success [11]. Intentional interference (e.g., jamming) degrades precision by increasing random errors, whereas spoofing reduces accuracy by introducing systematic biases, collectively compromising the performance of RTK systems [12]. Disruptions in GNSS services can degrade the accuracy of flight state estimation, potentially leading to navigation failure, system crashes, or even structural damage [13]. As illustrated in Fig. 1, GNSS interference can induce UAV heading errors, position deviations, and uncontrolled crashes [14]. In swarm operations, such interference may also induce relative position shifts within swarms, increasing the risk of intervehicle collisions [15].

A robust and reliable navigation system is essential for the successful execution of UAV missions (e.g., agriculture, logistics, and patrols). UAV navigation performance is often degraded in urban GNSS-denied environments. However, intentional interference further increases risk by jeopardizing the UAV platform itself and endangering nearby personnel and infrastructure, particularly in military operations [11]. Particularly concerning is the fact that low-cost software-defined radio (SDR) platforms, such as HackRF One, can generate interference capable of severely disrupting the commercial GNSS receivers commonly used on UAVs [16]. Consequently, countries are strengthening legislation against GNSS interference (e.g., the FCC's jamming device ban [17] and the European Aviation Safety Agency's Easy Access Rules [18]). The latest ICAO Annex 10, released in 2024, formally introduced critical GNSS safety provisions for UAV operations. Notably, it established technical criteria for navigation integrity alerts triggered by interference [19]. Given the growing dependence on UAVs across various fields, developing robust countermeasures against such intentional interference is paramount.

Several studies of UAV satellite navigation safety and interference countermeasures have been conducted, as summarized in Table I. Rugo et al. [22] and Hadi et al. [24] surveyed the cybersecurity threats faced by UAVs from hardware and software perspectives. Additionally, researchers [29] and [30] analyzed threats at the overall UAV system level on the basis of an analysis of real incident cases. Focusing specifically on UAV swarms, Wang et al. [27] analyzed security attacks from a data link perspective. In addition to investigating specific interference types, such as jamming, spoofing, and data tampering [21], [25], and [28], Burbank et al. [26] extensively analyzed intentional interference targeting UAV GNSS receivers, particularly jamming and spoofing attacks. With respect to interference countermeasures, prior surveys had distinct focuses and limitations. Although Gyagenda et al. [23] explored alternative sensor-based navigation in GNSS-denied environments, they did not address the core challenge of maintaining GNSS availability under active interference. Conversely, Morales et al. [20] provided a systematic countermeasure framework, encompassing tasks such as detection and identification. In addition, Jiang et al. [31] further analyzed technical categories such as array antenna and signal encryption-based methods. Nevertheless, these studies lacked analyses of emerging threats and AI-driven countermeasures. More importantly, they ignored algorithm performance under specific UAV constraints.

Collectively, existing studies have three limitations: *i)* Insufficient attention to the novel navigation interference faced by UAVs in application scenarios. In-depth analyses of various types of navigation interference and the corresponding effects on UAVs in practical contexts are lacking, particularly in terms of the summary of emerging threats. *ii)* Limited cross-method analysis for evaluating the techniques used to combat GNSS jamming and spoofing tailored for UAVs. Current research lacks a comparative analysis of countermeasures tailored specifically to jamming versus spoofing, and technology selection strategies tailored to specific UAV types have not been sufficiently explored. *iii)* Inadequate identification of challenges from platform resources to strategic responses. Previous studies generally summarized the relevant technical challenges without providing comprehensive anti-interference design insights for enhancing the safety of the GNSS for UAV systems.

To bridge the current research gaps, our survey systematically reviews existing detection and mitigation strategies for GNSS jamming and spoofing in UAV navigation over the past five years. We analyze, in particular, the shortcomings

TABLE I
SUMMARY OF SATELLITE NAVIGATION SAFETY RESEARCH FOR UAVS

Reference	Years	Contents	Contributions
[20]	2019	Taxonomy of interference types and models: • Jamming (e.g., AM, Chirp, and Pulse) • Spoofing (e.g., Meaconing and Intermediate spoofing)	Overview of interference countermeasures: • Detection • Identification • Localization • Suppression
[21]	2021	Taxonomy of cyberattacks on UAVs: • Channel jamming • Message attack (interception, deletion, injection, and spoofing) • On-board system attack	Classify attacks based on their attack entry points: • Radio channels • Messages • On-board systems.
[22]	2022	Review of cyber-security threats of UAVs: • Physical layer attack • Sensors attack	A detailed gap analysis of threat solutions: • Overload to sensors • Risks to supply chain • Vulnerabilities of communication
[23]	2022	Multisensor alternatives to address GNSS failure: • Inertial • Visual • LiDAR	Current state of GNSS-independent navigation solutions.
[24]	2023	Systematic division of security issues of UAVs: • Software • Hardware • Communication	Discussion about emerging technologies: • Blockchain usage • Machine learning • Intrusion detection
[25]	2024	Taxonomy of cyberattacks on UAVs: • GPS spoofing • Jamming • Malware • Data tampering	Analysis of open security challenges in UAV: • Standardization for vulnerability testing • Extensive deployment and scalability
[26]	2024	Taxonomy of factors for a GPS-disrupted environment: • Multipath • Unintentional interference • Jamming • Spoofing	Overview of detection and mitigation techniques: • Signal statistics-based • Antenna array-based • Machine learning-based
[27]	2024	A comprehensive review on the security of UAV swarm networks: • Denial-of-service attacks • Man-in-the-middle attacks	Introduction of security technologies to address attacks: • Cryptography • Blockchain
[28]	2024	A detailed category from the view of cyberspace security: • Spoofing attacks • Reply attacks • Jamming attacks • Denial-of-service (DoS) attacks	Countermeasures are categorized on the basis of the UAV system architecture: • Software-based • Hardware characteristic-based • Communication mechanism-based
[29]	2025	A systematic analysis of multifaceted cybersecurity threats: • Communication links • Navigation subsystems • Onboard controllers • Ground control stations	Emerging directions to inspire robust and adaptive security architectures: • Blockchain integration • Federated learning • Quantum-resistant cryptographic
[30]	2025	A detailed examination of RFI in UAV systems based on real-world incidents and simulated impacts: • GNSS systems • Altimeters • Instrument Landing Systems	Comparative insights into mitigation strategies: • Regulatory practices • Spectrum filters • Shielding architectures • Dynamic UAV sensing systems
[31]	2025	A comprehensive review of the classification of GNSS interference: • The principles and impacts of jamming and spoofing	Strength analysis of various anti-interference technologies: • Multiantenna-based • Signal encryption
Our work		a) A comprehensive discussion of interference: • Separate analysis of the principles and impacts for jamming and spoofing • Introduction of emerging interference (e.g., adaptive interference, covert interference, and multidimensional interference) b) Techniques for interference detection and mitigation: • Signal processing • Array antennas • Artificial intelligence	a) Evaluating metrics and advice for selecting countermeasures: • Detection and identification • Mitigation and suppression b) Multilevel framework in response to current challenges for future development: • Signal reception improvements • Algorithmic improvements • System advancements

of current countermeasures and the challenges associated with considering size, weight, and power (SWaP) constraints.

A. Contribution

The key contributions of this survey can be summarized as follows.

- We conduct a detailed analysis of GNSS interference specific to medium-scale UAVs on the basis of real-world scenarios and case studies. In addition to conventional interference, we specifically summarize the emerging threats and review the current countermeasures adopted by UAVs in different application scenarios.
- We separately classify countermeasures for jamming and spoofing and review recent advances in interference detection and mitigation, with comparative analysis to elucidate trade-offs across approaches. We subsequently

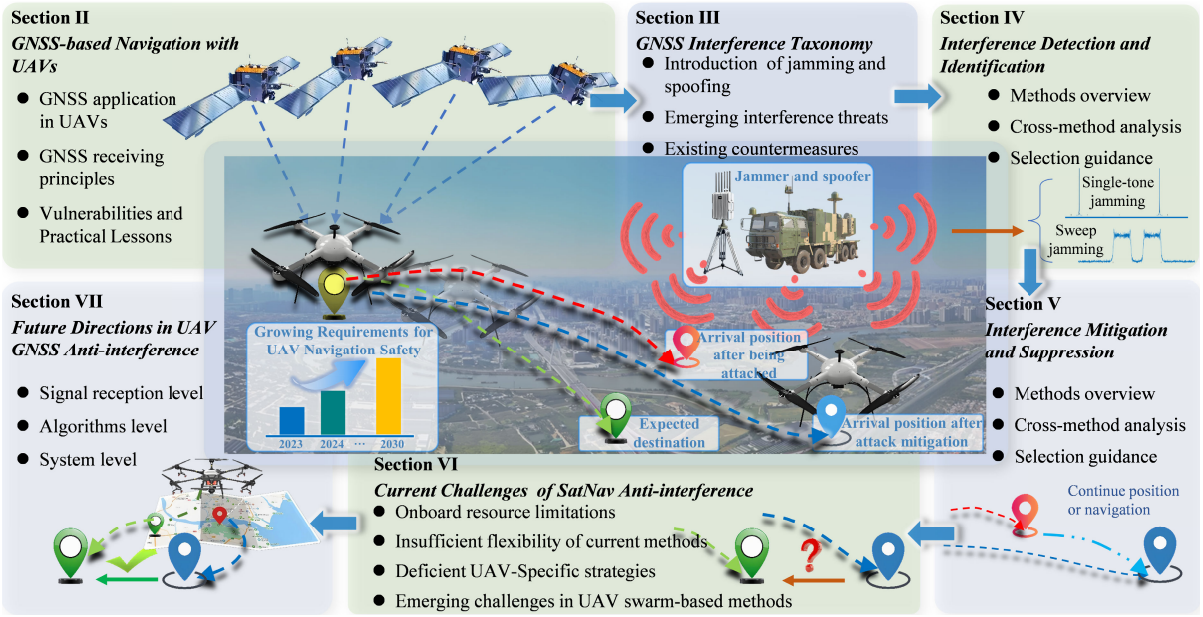


Fig. 2. Survey organization and sectional overview of GNSS anti-interference research for UAV navigation.

TABLE II
TYPICAL ROTORCRAFT UAV TYPES AND APPLICATION SCENARIOS

Types	Maximum takeoff weight	Specific scenarios	Navigation systems	Risks faced by navigation systems
FPVs	≤ 5 kg	Racing, filming, and emergency searches	Low-cost GPS and visual navigation	Data link jamming and ambient light limitations
Small UAVs	5 kg to 25 kg	Disaster rescue, power inspection, and environmental monitoring	Single-frequency GPS/Beidou satellite navigation, Inertial Measurement Unit (IMU), visually assisted localization	GNSS spoofing, Urban multipath effects
Medium UAVs	25 kg to 150 kg	Logistics distribution, precision agricultural, target positioning and tracking	Multiconstellation and multifrequency GNSS, dual-antenna RTK	GNSS jamming, GNSS spoofing
Large UAVs	>150 kg	Large-scale logistics transportation and material delivery	Anti-interference GNSS receiver and multisource fusion navigation	Military GNSS jamming and GNSS covert spoofing

perform semiquantitative evaluations to provide practical selection guidelines for diverse UAV application scenarios. Special attention is given to AI-based approaches, with a critical analysis of their effectiveness in different learning paradigms under several constraints.

- Furthermore, we identify the key challenges associated with current countermeasures, spanning multiple levels of emerging threats and resource limitations, and analyze the relationships among these challenges. On the basis of this analysis, we propose a hierarchical framework that enhances signal reception robustness, algorithmic adaptability, and system-level collaboration to provide actionable strategies for next-generation UAV navigation security.

B. Survey Structure

As illustrated in Fig. 2, this survey is organized as follows. Section II introduces the application of satellite navigation with UAVs and the receiving and processing of GNSS signals. Section III provides an overview of jamming and spoofing and briefly summarizes existing countermeasures. Sections IV and V delve into detection and mitigation for jamming and spoofing. Section VI highlights the current challenges in UAV anti-interference navigation. In Section VII, future research directions are proposed. Finally, Section VIII summarizes this survey.

II. GNSS-Based Navigation With UAVs

A. Evolution of GNSS Applications in UAV Navigation

As indicated in Table II, medium-sized UAVs are extensively utilized in industrial applications along with certain small UAVs. Capable of carrying mission payloads, these UAVs perform complex tasks such as logistics distribution and target positioning. Accurate navigation and positioning are essential for completing such missions and maintaining real-time motion state awareness. Moreover, the security of the

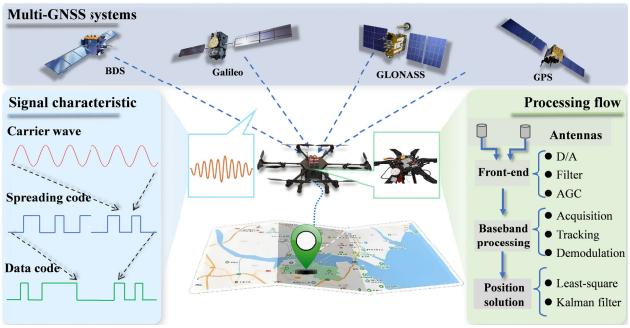


Fig. 3. GNSS signal structure and reception flow. Navigation receivers onboard UAVs acquire GNSS signals from multiple satellite constellations. The receiver sequentially processes signals through the RF front end, baseband processing, and ultimately position solution.

navigation system critically affects the effectiveness of mission execution, especially under SWaP constraints when operating in an interference environment.

UAV navigation technologies have progressed from traditional inertial and satellite navigation to visual and LiDAR navigation and further to relative positioning using UWB and 5G signals [32]. While alternative technologies such as INS [10] and visual SLAM [33] can support short-term navigation, GNSS remains the only viable solution for providing precise, absolute positioning and heading reference data over extended periods.

The role of satellite navigation (SatNav) in UAV operations has evolved significantly. Initially, SatNav was primarily used for basic positioning to provide the UAV location and velocity. The transition from single-point positioning to relative positioning (i.e., RTK technology) has enabled UAVs to achieve high-precision and reliable positioning. RTK employs a base station to process GNSS signal correction data and transmits these data to UAVs in real time, effectively compensating for signal delays and achieving centimeter-level accuracy. This capability is particularly valuable in high-precision fields such as surveying and agriculture [34]. In addition, carrier phase differences across multiple antennas can be exploited to estimate baseline variations on the basis of dual-antenna RTK, enabling high-precision attitude determination [35]. This capability significantly enhances the accuracy of UAV flight status monitoring.

The advent of multi-GNSS constellations has further improved navigation robustness by providing redundant signal sources. By exploiting the complementary strengths of different systems, combined measurements enhance integer ambiguity resolution (AR) in relative positioning [36]. For instance, the joint use of GPS L1 and Galileo E1 signals has been shown to improve AR success rates and attitude estimation accuracy [37]. In challenging environments such as urban areas, compared with single-system solutions, multi-GNSS integration, which benefits from increased satellite availability and improved geometric diversity, delivers superior positioning and attitude performance [38].

B. Principles of GNSS Signal Reception

1) Signal Characteristics: As illustrated in Fig. 3, the GNSS encompasses multiple satellite constellations. These systems differ in signal frequency and modulation but share similar signal structures based on direct-sequence spread spectrum (DSSS) technology. DSSS modulates the signal using a high-rate spreading code, enabling code-division multiple access [39].

The GNSS signal can be mathematically modeled as follows:

$$s(t) = A \cdot D(t) \cdot C(t) \cdot \cos\big(\pi\,(f_c + \Delta f)\,t + \phi(t)\big), \qquad (1)$$

where $s(t)$ denotes the transmitted signal, A represents the amplitude determined by transmitter power and path loss, $D(t)$ is the navigation data bitstream ($\pm$ 1), and $C(t)$ is the spreading code sequence. The spreading and navigation data codes are modulated onto the carrier wave to form a composite GNSS signal. This structure ensures the precise measurement of signal propagation delay through code phase tracking. Such a code phase corresponds to the satellite-to-user distance and is the fundamental input for positioning calculations [40]. The carrier frequency f_c (e.g., 1575.42 MHz for GPS L1) is offset by a Doppler shift Δf because of relative satellite-receiver motion, and $\phi(t)$ accounts for aggregate phase noise from oscillator instabilities and atmospheric effects.

GNSS signals travel over 20 000 km through free space before they reach user equipment. Along this path, they traverse atmospheric layers such as the ionosphere and troposphere and experience significant attenuation because of path loss [41]. Consequently, the received signal power at the antenna can be as low as -160 dB $\cdot$ W, much lower than the thermal noise level. This inherent signal weakness makes the GNSS highly vulnerable to various forms of interference.

2) Processing Flow of Signal Reception: From antenna reception to baseband demodulation, each component of the GNSS receiver is designed to reliably process extremely weak signals [42]. As shown in Fig. 3, the RF front-end receives navigation signals via a multiband antenna. These signals are downconverted to an intermediate frequency via bandpass filtering and sampling. They are then digitized with an analog-to-digital converter (ADC) for baseband processing.

The baseband processing stage encompasses signal acquisition, tracking, and data demodulation. This process is used to sequentially extract the pseudorange, carrier phase, and Doppler shift information from the navigation signals [43]. Finally, these measurements are used to calculate the receiver's position, velocity, and other information via least squares or Kalman filtering methods [44].

The resulting navigation solution is then transmitted in real time to the UAV's flight control system. Using these data along with mission profiles and control algorithms, the system generates flight commands for attitude control, speed regulation, and path planning [45].

C. Vulnerabilities and Practical Lessons

GNSS signals used in UAV navigation are inherently vulnerable to interference, particularly in complex electromagnetic environments. These vulnerabilities, combined with the increasing sophistication of intentional interference, underscore the urgent need for effective countermeasures to ensure safe and reliable UAV operations.

1) Inherent Vulnerabilities of the GNSS on UAVs: The SatNav system on UAVs is vulnerable because of factors ranging from signal characteristics to platform limitations. This vulnerability manifests in three main aspects:

- **Signal Characteristics**: The GNSS signals employed by UAVs typically have open signal architectures and exhibit extremely low power levels at receivers.
- **Hardware Limitations**: The adaptive adjustment ability of the GNSS receiver hardware is limited (e.g., insufficient adjustment capacity for automatic gain control (AGC) and restricted bandwidth of the tracking loop).
- **Platform Constraints**: UAV platforms are constrained by payload and computing resources, making it challenging to adopt effective anti-interference techniques (e.g., large antenna arrays and complex algorithms).

Consequently, when high-power barrage jamming occurs at the RF front end, hardware with a limited adjustment range becomes saturated and operates in the nonlinear region. Moreover, the open civil GNSS signal structure makes it difficult for the receiver to distinguish between authentic signals and fake spoofing signals with identical formats. These issues highlight an inherent security vulnerability of UAV GNSS systems to both jamming and spoofing attacks.

2) Reality and Harmfulness of Interference: UAVs frequently operate in electromagnetically contested environments, where the growing sophistication of electronic warfare systems has led to a wide range of interference sources. Advanced systems can simultaneously employ multiple interference strategies to disrupt satellite navigation signals [46]. For instance, the use of extensive electronic jamming equipment during the Russia-Ukraine conflict to conduct large-area GPS spoofing caused Russian UAVs to obtain incorrect position information [47]. Concurrently, reports indicate that in the first half of 2024, more than 1600 instances of GNSS interference were reported by civil aviation in the Baltic region, affected by battlefield electronic warfare [48].

Furthermore, research on aircraft operational capabilities in complex electromagnetic environments has demonstrated that UAVs with limited anti-interference capabilities struggle to reliably follow predefined mission plans under such conditions [49]. Additionally, current software-defined radio (SDR)-based UAV management systems can generate both jamming and spoofing signals, enabling various attack methodologies that can disrupt the normal operation of satellite navigation systems on UAVs [46].

These real-world cases sufficiently demonstrate that in cases with malicious navigation interference, UAVs with limited anti-interference capabilities struggle to maintain normal operation of their onboard navigation systems. Consequently, such systems fail to provide the reliable position and orientation data required for effective flight path planning.

3) Specific Standards and Insights Into UAV Operations: To enhance the operational safety of UAVs in interference-prone environments, aviation-grade safety standards have been introduced internationally. For instance, the Radio Technical Commission for Aeronautics (RTCA) has published a series of standards [50], such as RTCA DO-373 and RTCA DO-292A. Besides, China has established its own framework of UAV safety standards including GB/T 38909-2020 and GB/T 38997-2020 [51], [52].

These standards indicate that enhancing UAV flight safety in interference environments is both an industry consensus and a mandatory requirement. Accordingly, anti-interference solutions must be compatible with the data link architecture of UAVs and the allocation constraints of onboard hardware resources.

Therefore, enhancing the interference resilience of UAV navigation systems is a critical priority for both military and civilian applications, particularly as reliance on GNSS continues to grow.

TABLE III
SUMMARY OF GNSS INTERFERENCE RESEARCH ON UAVS IN RECENT YEARS

Types	Literature	Time	Specific patterns
Jamming	[53]	2024	Noise jamming, sweep jamming, tone jamming, follower jamming, smart jamming
	[54]	2024	CWI jamming
	[55]	2024	Tone jamming, swept jamming, protocol-aware jamming
	[25]	2024	No specific patterns
	[24]	2023	No specific patterns
	[22]	2022	Partial-band jamming
	[46]	2022	Barrage jamming, tone jamming, sweep jamming, successive pulses jamming
	[56]	2021	Noise jamming, follower jamming, tone jamming, chirp
	[57]	2020	Co-channel jamming, the mixer sub channel jamming
	[58]	2019	No specific patterns
Spoofing	[53]	2024	Static spoofing, dynamic spoofing
	[59]	2024	Position spoofing
	[60]	2024	Position spoofing
	[55]	2024	Generated spoofing
	[25]	2024	Path spoofing, location spoofing
	[61]	2023	Generated spoofing
	[24]	2023	Hijacking, position spoofing
	[22]	2022	Hijacking, generated spoofing
	[46]	2022	Generated spoofing
	[56]	2021	Sensor spoofing, Meaconing, SCER
	[62]	2021	Meaconing, Fabrication, time spoofing, location spoofing, time and phase compensated spoofing
	[63]	2021	Generated spoofing, multi-UAVs spoofing
	[64]	2020	Direction spoofing
	[58]	2019	Repeater spoofing, generated spoofing
	[65]	2019	Soft GPS spoofing, hard GPS Spoofing

III. GNSS INTERFERENCE TAXONOMY

UAVs are being increasingly exposed to various types of interference. As summarized in Table III, intentional interference has become the dominant concern in UAV navigation research [22]. Such interference implemented via human control can severely disrupt UAV flight operations [56]. This section focuses on two primary types of intentional interference, jamming and spoofing, detailing their principles, classifications, and impacts on UAV navigation systems.

TABLE IV
SUMMARY OF PRINCIPLES AND IMPACTS FOR TYPICAL JAMMING

Types	Models	Impacts		
		RF front-end	Acquisition & tracking	Positioning
CWI	$J(t) = A_j \cdot \sin(2\pi f_j t + \phi_j)$	• AGC fails, and signal gain cannot be regulated; • The CNR decreases because of noise introduction; • Front-end devices produce nonlinear effects because of excessive operation.	• The correlation peak is submerged by noise; • Jamming signals generate an abnormal jitter code phase and a carrier phase; • The abnormal deviation caused by interference causes the loop to lose its lock.	• Loop loss reduces the number of visible stars used for positioning; • Jamming noise increases measurement error; • Position cannot be obtained when jamming is severe.
Multitone jamming	$J(t) = \sum_{n=1}^{N} A_n \cdot \sin(2\pi f_n t + \phi_n)$			
Chirp jamming	$J(t) = A_j \cdot \sin\left(2\pi\left(f_0 t + \frac{1}{2}kt^2\right) + \phi_j\right)$			
Pulse jamming	$J(t) = A_j \cdot \sin(2\pi f_j t + \phi_j) \cdot \sum_{m=-\infty}^{\infty} \text{rect}\left(\frac{t - mT_p}{\tau}\right)$			
Partial-band Jamming	$J(t) = A_j \cdot \text{rect}\left(\frac{f - f_j}{B_j}\right) \cdot \sin(2\pi f_j t) \otimes n(t)$			

Symbol Definitions:
t: Time variable (s)
ϕ_j: Initial phase (rad)
f_n: Frequency of nth tone (Hz)
k: Sweep rate (Hz/s)
m: Pulse index ($m \in \mathbb{Z}$)
$\otimes$: Convolution operator
A_j: Jamming amplitude
N: Number of tones
ϕ_n: Phase of nth tone
τ: Pulse width (s)
rect(x): Rectangular function
$n(t)$: Additive noise
f_j: Center frequency (Hz)
A_n: Amplitude of nth tone
f_0: Initial sweep frequency (Hz)
T_p: Pulse repetition period (s)
B_j: Jamming bandwidth (Hz)

A. Jamming

1) Principles and Characteristics: Jamming involves transmitting high-power signals to overwhelm or mask GNSS signals [66]. Owing to the inherently low received power of navigation signals, even low-power jammers can be highly effective. For instance, 1 W jamming can disrupt GNSS reception within a 30 km radius [67]. For low-altitude platforms such as UAVs, only minimal jamming power is needed to degrade or completely disrupt navigation capabilities. As summarized in Table IV, jamming signals can be categorized into several types on the basis of their spectral and temporal characteristics [68].

- **Continuous wave interference (CWI)**: Also known as single-tone jamming, a narrowband sinusoidal signal near the GNSS carrier frequency is transmitted, concentrating energy at a specific point [69].
- **Multitone jamming**: Comprising multiple sinusoidal tones, it results in wider spectral interference than CWI does [70].
- **Chirp jamming**: Sweeping through a range of frequencies, it covers a wide bandwidth in a short time. This reduces the effectiveness of time- or frequency-domain mitigation algorithms [71].
- **Pulse jamming**: Composed of high-power and short-duration pulses, it has a narrow bandwidth and high energy density. Its duty cycle can be adjusted to disrupt various signal types [72].
- **Partial-Band jamming:** It injects noise into a specific subband of the GNSS signal spectrum, selectively degrading signal quality within that frequency range.

Among the aforementioned types of jamming, CWI, multitone and partial-band jamming are classified as types of narrowband jamming because of their concentrated energy within a limited frequency range. Once within the navigation signal bandwidth, it can cause the navigation receiver's channel to saturate or overflow [73]. Broadband jamming, such as chirp jamming, covers a wide spectrum range with complete submergence of the signal band [74].

2) Impact of Jamming: Owing to its high power relative to that of GNSS signals, jamming significantly decreases the carrier-to-noise ratio (CNR), leading to signal acquisition failure or tracking loss. These ultimately degrade positioning accuracy or even disable navigation functionality [71]. The specific effects of jamming on receivers can be categorized as follows.

- **RF Front-End**: Jamming primarily affects the receiver's front end by significantly reducing the CNR. An increase in the Jamming-to-Noise Ratio (JNR) from $55\ \text{dB} \cdot \text{Hz}$ to $92\ \text{dB} \cdot \text{Hz}$ can lead to a 15 dB degradation in the CNR [75]. Besides, when the interference power exceeds the dynamic range of AGC, the signal becomes clipped or distorted because of quantization limitations [12].
- **Signal acquisition and tracking**: Jamming-induced CNR degradation directly impairs the receiver's ability to acquire and track GNSS signals [76]. Specifically, a low CNR reduces the prominence of the correlation peak, making it difficult to distinguish the authentic signal from noise [77]. During tracking, jamming introduces jitter in both the code and carrier phases, leading to deviations in the discriminator outputs [67].
- **Positioning**: Jamming impacts positioning solutions in two ways: by reducing visible satellites and increasing measurement errors. Under strong jamming, front-end saturation may prevent the receiver from maintaining lock on sufficient satellites. For example, Borio et al. [75] reported that at Jamming-to-Signal Ratios (JSRs) of 65 dB and 70 dB, a u-blox 5H receiver achieved valid positioning only 16% and 14% of the time, respectively.

These jamming-induced impairments also affect the application of the GNSS to UAVs. For instance, RTK reference stations may fail to compute fixed solutions under jamming conditions, preventing correction data dissemination.

TABLE V
SUMMARY OF PRINCIPLES AND IMPACTS FOR TYPICAL SPOOFING

Types	Models	Impact		
		RF front-end	Acquisition & Tracking	Positioning
Generated spoofing	$J_{\text{gen}}(t) = A_j \cdot D_{\text{fake}}(t) \cdot C_{\text{fake}}(t) \cdot \cos(2\pi f_c t + \phi_j)$	• False signals occupy the processing channel; • AGC reduces the effective gain because of deception signal energy.	• The receiver mistakenly captures the wrong correlation peak; • The loop tracks onto false signals instead of authentic signals; • It introduces phase discrimination error in measurements.	• The position output deviates because the measurement value is incorrect; • The position and flight direction are tampered with by deceptive signals; • The flight path deviates from the planned route.
Meaconing	$J_{\text{relay}}(t) = \alpha \cdot S(t-\tau) \cdot \cos(2\pi(f_c + \Delta f)t + \phi_j)$			
Asynchronous spoofing	$J_{\text{async}}(t) = A_j \cdot D_{\text{fake}}(t) \cdot C(t-\theta_c) \cdot \cos(2\pi(f_c + \Delta\phi)t + \phi_j)$			
Synchronous spoofing	$J_{\text{sync}}(t) = A_j \cdot D_{\text{fake}}(t) \cdot C(t) \cdot \cos(2\pi f_c t + \phi_0)$			

Symbol Definitions:
A_j: Jamming amplitude
$D_{\text{fake}}(t)$: Fake navigation data
$C_{\text{fake}}(t)$: Fake PRN code
$C(t)$: Authentic PRN code
ϕ_0: Synchronized carrier phase
f_c: Carrier frequency (e.g., GPS L1)
α: Relay gain ($\alpha > 1$)
$S(t)$: Authentic signal ($D(t) + C(t)$)
θ_c: Code phase offset (chips)
ϕ_j: Initial phase offset
τ: Relay delay (for fake pseudorange)
Δf: Doppler shift adjustment
$\Delta\phi$: Carrier frequency offset

Simultaneously, broadband jamming can eliminate frequency diversity across multi-GNSS constellations, undermining redundancy. Furthermore, the loss of carrier-phase continuity severely degrades the attitude determination accuracy, which is critical for UAV flight control.

B. Spoofing

1) Principles and Characteristics: Spoofing involves transmitting counterfeit GNSS signals that mimic authentic signals in structure, power, and timing, thereby misleading the receiver into computing a false position or time [78]. As shown in Table V, spoofing can be categorized by signal source or synchronization strategy [79]:

- **Generated spoofing**: This refers to artificially synthesizing GNSS-like signals using known signal structures. [80]. However, this requires prior knowledge of the structure of the authentic signal.
- **Meaconing**: Authentic GNSS signals are intercepted and retransmitted with a time delay [81]. This approach can target encrypted military signals via code estimation and replay (SCER) attacks [82].
- **Asynchronous spoofing**: High-power fake signals are transmitted to force the receiver to lose lock and relock onto the spoofed signal [83].
- **Synchronous spoofing**: The spoofing signal is aligned with the authentic signal in terms of time and frequency, allowing both to be tracked simultaneously. The spoofing signal is gradually amplified to take over the tracking loops [84].

2) Impact of Spoofing: Spoofing can hijack a UAV by manipulating its perceived position and velocity. Its low cost and stealthy nature make it a significant threat [65]. As experimentally validated in [63], controlled delay adjustments can hijack multiple UAVs simultaneously within a targeted area. The impact of such attacks on navigation can be summarized as follows.

- **RF Front-End:** Spoofing signals consume additional correlator resources and may exceed the power of authentic signals, causing AGC instability and reducing the number of available processing channels.
- **Acquisition and Tracking:** A spoofing signal just 2 dB stronger than the authentic signal can dominate the correlation peak [85]. It introduces bias in pseudorange and carrier-phase measurements. PLL discriminators may also be misled to lock onto the false signal.
- **Positioning:** Biases in pseudorange and carrier phase measurements lead to significant deviations in positioning solutions [64]. These deviations enable control over the position and flight direction of UAVs by precisely manipulating the spatiotemporal characteristics of fake signals [65].

Spoofing introduces counterfeit pseudorange and carrier-phase measurements, compromising carrier-phase-dependent techniques such as the RTK and attitude determination. Notably, progressive-phase spoofing induces deviations in the heading of the UAV, which can lead to unauthorized control. Furthermore, spoofers simultaneously fabricate multisystem signals by leveraging the geometric consistency between signals to enhance deceptive credibility.

C. Emerging Interference Threats

Beyond traditional jamming and spoofing, modern GNSS face emerging threats characterized by adaptive, stealthy, and multidimensional coordination. These techniques significantly influence the effectiveness of interference and operational efficiency.

1) Adaptive Interference: The parameters of adaptive interference can be dynamically adjusted on the basis of the target behavior or environment. Various intelligent attack paradigms tailored for specific scenarios have been developed. For instance, Chang et al. [86] proposed a scenario-constrained dynamic spoofing method. This technology can be used to

evaluate GNSS skyplots in real time to identify vulnerable periods in the navigation process. For example, when the target leaves the tunnel in an urban environment, it relies on the GNSS for positioning measurement and correction. By launching spoofing attacks during these critical windows, the method significantly increases the success rate from less than 40% (with traditional methods) to approximately 75% and can rapidly induce significant lateral deviations in the target at high-risk locations. Similarly, He et al. [87] established a simulation platform capable of perceiving UAV positions. By utilizing a GPS signal simulator, they adaptively adjusted spoofing signals, successfully causing two drones to misinterpret their respective positions. This led to a collision at a predetermined point, demonstrating the concrete threat of such attacks in instigating physical impacts.

Furthermore, coordinated interference strategies targeting UAV swarms exhibit even greater complexity. Ceccato et al. [88] designed a formation spoofing method for drone clusters. Using a multitransmitter antenna array, the entire swarm simultaneously receives spoofing signals mimicking more than four satellites. This approach lures the entire formation toward a false destination without disrupting the internal relative positioning, thus avoiding the triggering of consistency checks and eliminating the need to track each UAV's trajectory individually. Additionally, Ma et al. [89] integrated radar detection with game theory and knowledge-driven deep reinforcement learning. They estimated the flight intent of UAVs (e.g., approaching, returning, or deceiving) to dynamically apply hybrid interference. This strategy maneuvers UAVs into a controllable area before capture tasks are implemented, showcasing the adaptive capability of interference across both temporal and strategic dimensions.

These studies indicate that adaptive interference represents a critical threat, as adjustments are made in real time on the basis of target assessment to induce navigation errors. The main detection challenge stems from the ability to continuously adapt strategies based on context-aware algorithms. This closed-loop adaptability makes it exceptionally difficult for static detection methods to distinguish interference from normal operational variations.

2) Covert Interference: Current research on covert spoofing focuses on evading detection mechanisms in advanced navigation systems. The core concept involves controlling the dynamic characteristics of spoofing signals within the insensitive range of receivers or fusion filters, thereby avoiding anomaly detection. One representative method is the targeted spoofing algorithm proposed by Gao et al. [90]. By analyzing the response patterns of UAVs to spoofing, they developed a multistep progressive attack that induces a -1.13° heading deviation within 670 s without triggering alarms. Geng et al. [91] targeted tightly coupled GNSS/INS systems and constructed a spoofing model constrained by innovation sequences and state estimation parameters. By adding pseudorange and pseudorange rate offsets, they gradually altered the system's positioning output. Their vehicle experiments achieved a spoofing position error of better than 1.01 m in 3D, and the success rate increased by 39%. Chen et al. [92] further formulated the problem as a constrained single-objective optimization problem. Using an improved genetic algorithm to adjust spoofing parameters in real time, they achieved spoofing convergence within 0.3 s for loosely coupled systems.

Research has extended from the signal layer to the system architecture layer, achieving deeper concealment by exploiting logical vulnerabilities within navigation systems. Jung et al. [93] analyzed the integration vulnerabilities between the state estimation layer (e.g., Extended Kalman Filter) and the planning layer (e.g., deep reinforcement learning for autonomous navigation). By directly tampering with the relative position and yaw angle inputs of the reinforcement learning system, they successfully induced UAVs to collide with obstacles. In addition, Geng et al. [94] targeted the system steady-state matrix and introduced velocity and attitude error constraints to optimize the signal model. Their vehicular experiments demonstrated a spoofing distance of 157.27 meters within 100 seconds, increasing the covert spoofing success rate by 13.64%.

Unlike adaptive interference, covert interference poses a profound threat because it specifically targets the integrated GNSS/INS system of UAVs. The primary threat lies in gradually and imperceptibly seizing control. This results in the accumulation of navigation drift while actively evading built-in integrity checks. The key detection difficulty stems from the design principle of this approach, where the spoofing signals are carefully optimized to be consistent with the target system's dynamic model and state update process.

3) Multidimensional Interference: The essence of multidimensional interference lies in the collaborative utilization of multiple physical domains or strategic dimensions of freedom to achieve jamming or spoofing effects unattainable in any single dimension. In terms of physical domain coordination, the work by Tang et al. [95] serves as a typical example. They employed a hybrid game-theoretic model to dynamically and holistically optimize the resources of distributed jammers across the spatial, temporal, spectral, and power domains. This approach achieves an optimal balance between interference efficacy and resource cost, enhancing the utility of multidimensional interference by more than 49.93%. From spatial and systemic dimensions, Geng et al. [96] conducted research leveraging the networking characteristics of UAV swarms. By implementing GNSS spoofing against key nodes, they induced coordinated heading deviations across the entire swarm.

Furthermore, the introduction of intelligent algorithms extends interference from the physical domain into the strategic and cognitive domains. Ma et al. [59] utilized deep reinforcement learning to enable an attack agent to adaptively select the optimal spoofing timing in the temporal dimension, successfully overcoming the challenge associated with an unknown target model in noncooperative scenarios. To enhance the concealment and complexity of spoofing strategies, they further integrated spatial information entropy and maximum entropy reinforcement learning. This approach optimizes the diversity and uncertainty of the action distribution in the strategy generation dimension, thereby promoting detection evasion based on behavioral pattern analysis [97]. These studies demonstrate that modern multidimensional

TABLE VI
INTERFERENCE THREATS AND TYPICAL COUNTERMEASURES FOR UAVS IN DIFFERENT SCENARIOS

Types	Scenarios	Threats	Constraints	Countermeasures	References
Commercial/ Consumer-grade UAVs	Aerial displays, aerial photography and urban inspections	Narrowband jamming, Meaconing	Cost and SWaP are extremely sensitive, requiring ease of operation.	Single-antenna-based signal processing, low-cost MEMS-INS combination	[98], [99], [100], [101]
Tactical/ Military-grade UAVs	Environmental reconnaissance and target identification	Broadband jamming, generated spoofing, adaptive and covert interference	Performance, reliability, and security are prioritized and are relatively insensitive to cost.	Anti-interference array antenna, multisensor deep fusion	[102], [103], [104], [105]

interference has evolved into a complex system confrontation problem requiring deep integration and coordination across the physical, behavioral, and decision-making layers.

Multidimensional interference represents a strategic-level threat. Intelligent algorithms autonomously learn optimal spatiotemporal attack strategies without prior knowledge of the target. This optimized diversity in attacks makes distinguishing static, model-based detectors from normal complex operational environments exceptionally challenging.

In summary, these emerging interference paradigms, characterized by dynamic adaptability, active concealment, and multidomain coordination, collectively constitute the most complex and challenging threats to current UAV GNSS navigation security. Their danger lies not only in causing navigation failure but, more critically, in their ability to hijack control authority.

D. Existing Countermeasures Against GNSS Interference

On the basis of the current typical types of GNSS interference, the interference threats and existing countermeasures faced by UAVs in civilian and military scenarios are analyzed in this section.

1) Interference Threats: As shown in Table VI, UAVs in different scenarios currently face various forms of interference.

- **Commercial/consumer-grade UAVs:** These low-cost drones are primarily used for civilian applications such as aerial displays and urban inspections. They commonly encounter interference aimed at drone dispersal for airspace control. The predominant interference methods used to target these UAVs are low-cost narrowband jamming and repeater-style spoofing.
- **Tactical/military-grade UAVs:** Deployed for military missions, including environmental reconnaissance and target identification, these drones operate in contested environments. They face more aggressive interference intended to disrupt flight or even destroy the platform. The primary threats include high-power broadband jamming, generated spoofing, and emerging threats such as adaptive and covert interference.

2) Examples of Typical Countermeasures: To restore the navigation function under GNSS interference in aforementioned scenarios, different countermeasures are adopted in practical.

a) For commercial/consumer-grade UAVs: When jamming causes a UAV to lose its GNSS signal, one countermeasure uses sensor data (e.g., acceleration, angular velocity, and timestamps) recorded during flight to estimate its current position and plan a safe return path, enabling secure homing postjamming [98]. Alternatively, GNSS threat simulators have been developed to evaluate a UAV's flight capabilities under simulated jamming and spoofing scenarios before actual missions. This proactive assessment approach aims to minimize potential equipment loss caused by in-flight interference [99]. In contrast to spoofing, techniques that involve data link technology are employed to encrypt and authenticate civil GNSS signals [100]. For UAV swarm operations, cooperative methods leveraging multi-UAV sensor fusion and consistency checks can detect spoofing, whereas multilateration techniques help reduce positioning errors [101]. Machine learning approaches have also been applied, using GNSS observations to predict spoofing-induced measurement errors and identify the interference status of a UAV [106].

b) For tactical/military-grade UAVs: The adoption of array antennas is a prevalent countermeasure. For instance, anti-jamming array antennas are deployed on platforms such as the US "Gray Eagle" UAV [102]. Physical shielding, such as enclosing the GNSS antenna in a metallic structure, can also be used to filter out low-elevation angle signals, thereby suppressing terrestrial jamming [103]. In the context of specialized attacks such as SCER, which target military signals, cryptographic authentication mechanisms are critical at the signal level. Representative implementations include the U.S. military's M-code [105] and Galileo's Open Service Navigation Message Authentication (OS-NMA) in the E1 band [104]. These approaches significantly mitigate the risk of navigation message tampering, ensuring reliable positioning solutions.

Notably, the navigation methods of commercial and consumer-grade UAVs follow a pragmatic design philosophy driven primarily by cost and SWaP constraints. This leads to a preference for software-based and sensor-fusion approaches, such as using existing IMU data for homing, preflight threat simulation, and machine learning models applied to standard GNSS observations. These improve robustness without adding specialized, costly hardware. Similarly, data-link authentication and cooperative swarm techniques build security upon existing communication modules and coordination protocols, avoiding standalone high-grade cryptographic receivers. These low-cost countermeasures fundamentally shape the development of anti-interference solutions in the civilian low-altitude economy.

TABLE VII
SUMMARY OF INTERFERENCE DETECTION AND IDENTIFICATION METHODS

Interference Types	Approach Categories	Specific Techniques	Operating Mechanisms	Technical Constraints	References
Jamming	Signal Processing Based	Time and frequency analysis	Different signals exhibit different distributions in the time-frequency domain.	It is difficult to balance the time-frequency resolution when selecting parameters.	[108], [109], [110], [111], [112]
		AGC detector	Jamming causes abnormal adjustment of AGC parameters.	It is difficult to distinguish between interference and environmental factors.	[113], [75], [114]
	Array Antenna Based	Array signal processing	Identification between jamming and GNSS signals based on different signal arrival angles and energies.	The detection performance is limited by the number of elements; specific types of jamming cannot be identified.	[115], [116], [117], [118]
	Artificial Intelligence Based	Machine learning	Detect and categorize based on signal features.	Manual feature extraction is required; Detection performance depends on the type and quantity of features.	[119], [120], [121], [122], [123]
		Deep learning	Automatically extract features and learn the relationships between these features.	Good performance is often associated with high network complexity and the consumption of a significant amount of computing resources.	[124], [125], [126]
Spoofing	Signal Processing Based	Signal quality monitoring	Deceptive signals cause distortion of the correlation function.	Detection is susceptible to multipath effects, and performance is affected by the power of deception signals.	[127], [128], [129], [130], [128], [131]
		Signal feature extraction	Utilize differences in signatures between a deception signal and an authentic signal.	Feature selection needs to be comprehensive and characterize signal characteristics.	[132], [133], [134], [135], [136]
		Radio frequency fingerprint	Rely on weak differences in the time-frequency characteristics of signals.	Extracting the RFF requires a large number of computations; A high CNR is required for reliable detection.	[137], [138], [139], [140], [141]
		Measurement monitoring	Detect anomalies in measurement values caused by deceptive signals.	Real-time detection is poor because of the lag caused by demodulation.	[142], [143], [144], [145], [146], [147]
	Array Antenna Based	Array signal processing	Detect based on the arrival angles of different signals.	It requires additional hardware equipment.	[148], [149], [150], [151], [152]
	Artificial Intelligence Based	Machine learning	Identify and classify signals by using signal characteristics	Classification effectiveness is affected by the number, type, and relevance of features.	[153], [154], [155], [156]
		Deep learning	The networks automatically extract and recognize signal features.	Complex networks can lead to high computational resource consumption.	[157], [158], [159], [160]
	Hybrid System Based	INS	Use inertial navigation measurements for anomaly detection.	Long-duration detection performance decreases because of INS-accumulated errors.	[161], [162], [163]
		Communication system	Detect the difference between the measured values obtained by communication signals and GNSS signals.	Communication signal transmission delay easily affects measurement accuracy.	[164], [165], [166]
		Visual system	Detect location anomalies using image position correlations.	The detection performance is easily affected by visible light in the environment.	[167], [168], [169]

Regardless of the application scenario, current responses to UAV GNSS interference follow two primary phases: detection and identification, which determine the presence and type of interference to guide subsequent actions; and mitigation and suppression, which aim to reduce or eliminate its impact on navigation performance. As illustrated in Fig. 4, this

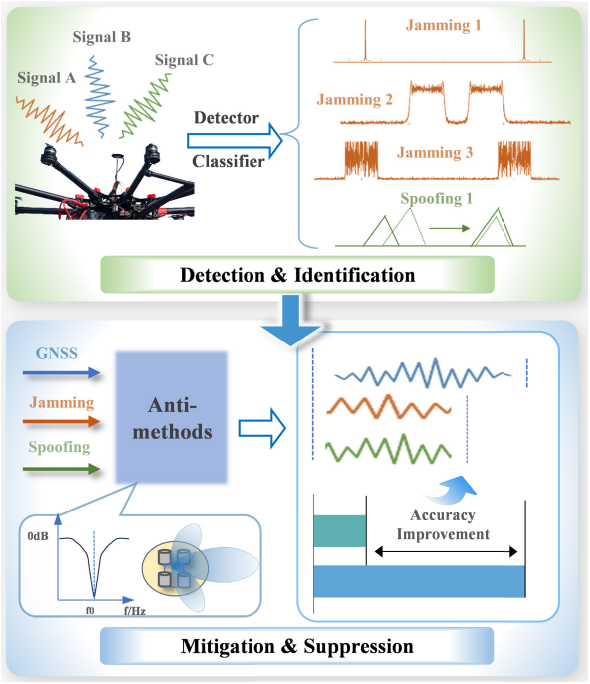


Fig. 4. Key stages of GNSS interference countermeasures. GNSS receivers first detect and characterize interference within composite signals. Interference is subsequently mitigated to increase positioning accuracy, which is compromised by interference effects.

process enables UAVs to obtain prior awareness of interference, upon which appropriate mitigation measures are applied. The following sections review state-of-the-art anti-interference techniques, supported by simulations and analyses to demonstrate their effectiveness.

IV. Interference Detection and Identification

Reliable detection and identification of interference are crucial for initiating effective countermeasures. Most modern receivers incorporate some basic interference monitoring capabilities [107]. Table VII summarizes existing detection methods for jamming and spoofing, outlining their mechanisms and practical limitations.

A. Jamming Detection and Identification

Jamming is typically detected by monitoring deviations in key receiver metrics such as CNR degradation, AGC instability, and changes in signal statistics [107]. These anomalies, observed at the signal processing stage, are fundamental for effective detection.

1) Signal Processing-Based Methods: These approaches detect jamming by analyzing changes in signal characteristics, such as time-frequency distribution, correlation peak shape, and energy level [121].

a) Time–frequency analysis: Jamming alters the time- or frequency-domain characteristics of received signals. Time-frequency transforms (e.g., the short-time Fourier transform (STFT) [108], wavelet transform (WT) and the Wigner–Ville distribution (WVD) [109]) can reveal abnormal energy patterns and be used to distinguish jamming signals from GNSS signals [110]. The typical time-frequency transform is defined as follows:

$$\mathrm{STFT}(t,\omega)=\int_{-\infty}^{\infty}x(\tau)w(t-\tau)e^{-j\omega\tau}\mathrm{d}\tau, \tag{2}$$

$$\mathrm{WT}(a,b)=\int_{-\infty}^{\infty}x(\tau)\frac{1}{\sqrt{a}}\psi\left(\frac{\tau-b}{a}\right)\mathrm{d}\tau, \tag{3}$$

$$\mathrm{WVD}(t,\omega)=\int_{-\infty}^{\infty}x\left(t+\frac{\tau}{2}\right)x^{*}\left(t-\frac{\tau}{2}\right)e^{-j\omega\tau}\mathrm{d}\tau, \tag{4}$$

where $x(t)$ denotes the input signal, t represents time, ω signifies frequency, and τ is a time-shift variable used in the integration process across these transforms. $w(t)$ represents the sliding window function in the STFT. a and b represent the scale and position parameters, respectively, and ψ is the mother wavelet in wavelet transform. In the WVD, $x^{*}(t)$ denotes the complex conjugate of the input signal.

Time-frequency (TF) analysis requires no additional hardware and can reveal both the timing and spectral content of jamming signals [111]. However, it involves a trade-off between time and frequency resolution, and its limited adaptability to rapidly changing interference characteristics may reduce detection performance in dynamic jamming scenarios [112].

b) AGC detector: Jamming can be detected by monitoring AGC levels, as interference-induced SNR changes are reflected in AGC behavior [113]. AGC behavior can be modeled as follows:

$$V_{\mathrm{AGC}}=K\cdot\log_{10}(P_n+P_j)+C, \tag{5a}$$

$$\Delta V_{\mathrm{AGC}}=|V_{\mathrm{AGC}}-V_{\mathrm{nom}}|>\gamma, \tag{5b}$$

$$\mathrm{SNR}_{\mathrm{eff}}=\frac{P_s}{P_n+P_j}, \tag{5c}$$

where V_{AGC} is the gain control voltage and P_n and P_j are the noise and jamming power, respectively. The parameter K signifies the AGC loop gain coefficient, while C represents a calibration constant determined during receiver characterization. The voltage deviation ΔV_{AGC} is the difference between the observed AGC voltage and its nominal value V_{nom} under interference-free conditions. γ is the detection threshold established through statistical analysis of false alarm probabilities. The effective $\mathrm{SNR}_{\mathrm{eff}}$ reflects the degradation in receiver sensitivity, where P_s indicates the desired satellite signal power.

To account for bandwidth normalization, the CNR (C/N_0) is used instead of the raw power. After accounting for C/N_0 variations caused by environmental factors, jamming detection becomes more effective [75]. When C/N_0 decreases, the AGC detector becomes as follows:

$$\left(\frac{C}{N_0}\right)_{\mathrm{eff}}=\frac{C}{N_0+J_0}, \tag{6a}$$

$$\Delta V_{\mathrm{AGC}}=K\cdot\left|\log_{10}\left[\frac{(C/N_0)_{\mathrm{nom}}}{(C/N_0)_{\mathrm{eff}}}\right]\right|>\gamma, \tag{6b}$$

where J_0 represents the interference power spectral density (W/ Hz), and N_0 is the thermal noise density. In addition to monitoring AGC and C/N_0 values, using their entropy as a detection threshold further reduces false alarms [114].

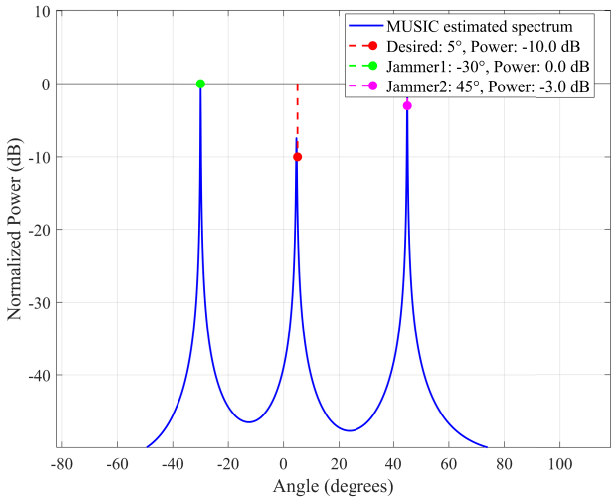
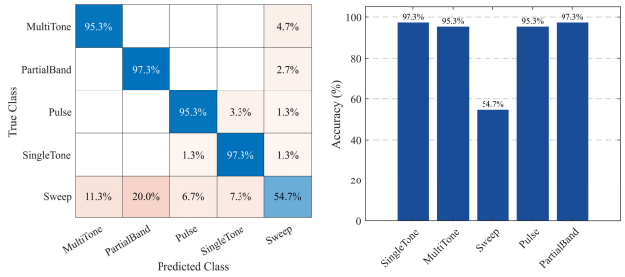


Fig. 5. DOA estimation using MUSIC algorithm in a four-element array antenna with one GNSS signal and two jamming sources.



(a) Normalized confusion matrix (b) Identification accuracy

Fig. 6. Jamming identification using an SVM with statistical features (RMS, mean amplitude, variance, kurtosis, and skewness) at an SNR $= -10$ dB.

In summary, both time-frequency analysis and AGC monitoring provide viable means for jamming detection, yet they present distinct trade-offs. TF analysis provides a detailed, feature-centric approach by transforming the signal to expose spectral-temporal anomalies and offers high diagnostic value for characterizing interference. Its fundamental trade-off involves time-frequency resolution and computational complexity. Its performance is also highly dependent on the chosen transform and parameters, making it less adaptable to dynamic jamming scenarios. Conversely, the AGC detector employs a hardware-centric, indirect approach by monitoring the receiver's internal gain control voltage. It outperforms other methods in terms of minimal computational overhead and easy integration but faces a critical trade-off between detection sensitivity and robustness to false alarms caused by natural signal power variations. This dichotomy positions TF analysis as a powerful diagnostic method for postprocessing or controlled environments, whereas the AGC detector serves as an efficient operational monitor for real-time and resource-constrained platforms.

2) Array Antenna-Based Methods: Spatial processing using antenna arrays enables the detection of jamming without relying on specific time or frequency features [115]. In this technique, the direction of arrival (DOA) of incoming signals is estimated, allowing for the identification and separation of jamming signals from GNSS satellite signals. As shown in Fig. 5, the classical multiple signal classification (MUSIC) algorithm uses eigenvalue decomposition of the received signal covariance matrix to distinguish signal and noise subspaces, enabling accurate DOA estimation [170]. MUSIC is illustrated as follows.

$$P_{\mathrm{MUSIC}}(\theta) = \frac{1}{\boldsymbol{a}^H(\theta)\boldsymbol{U}_N\boldsymbol{U}_N^H\boldsymbol{a}(\theta)}, \tag{7a}$$

$$\hat{\theta} = \arg\max_{\theta} P_{\mathrm{MUSIC}}(\theta), \tag{7b}$$

where $\boldsymbol{U}_N$ is the noise subspace, $\boldsymbol{a}(\theta)$ is the steering vector, and $\hat{\theta}$ is the estimated angle of jamming.

Traditional algorithms are slower in performing exhaustive search for signal DOA. To address this issue, Osman et al. [116] proposed the fast orthogonal search (FOS) algorithm to increase the speed of DOA estimation. The FOS approach not only improves estimation accuracy and robustness under low SNRs but also effectively separates closely spaced signals. In addition, the FOS algorithm enhances interference nulling and reduces the distortion of GPS signals when jamming and satellite signals arrive from similar directions [117].

Besides regular array antennas, jamming detection can also be performed by leveraging the different physical orientations of antennas. Sharifi et al. [118] used omnidirectional antennas installed on the drone body to receive mixed signals of satellites and jamming, as well as downward sloping directional antennas to only receive jamming from the ground. By comparing the power distributions, they achieved low cost and low complexity without the need for a full antenna array.

In summary, the above methods represent a fundamental trade-off between precision and practicality in spatial jamming detection. The classic array-based algorithms (e.g., MUSIC and FOS) utilize the full spatial sampling of an antenna array to achieve high-resolution DOA estimation, enabling the precise discrimination and nulling of jammers. This capability, however, comes at the cost of significant computational complexity and hardware requirements. In contrast, methods employing physically oriented antennas forgo precise DOA estimation for a simpler, hardware-intuitive comparison of power levels between differently pointed antennas. This approach offers a low-cost, low-complexity solution suitable for binary detection of ground-based jammers but at an inherently coarser spatial resolution. The choice thus pivots on whether the system prioritizes high-fidelity spatial filtering or minimalistic, cost-effective awareness.

3) Artificial Intelligence-Based Methods: AI methods can effectively utilize the features of received signals to classify interference, reducing reliance on manual processing [122]. The main AI-based approaches for jamming detection are summarized in Table VIII.

a) Machine learning (ML): Traditional machine learning approaches focus primarily on supervised learning, including classification, regression, and ensemble methods. Typical classifiers include support vector machines (SVMs), K-nearest neighbor (KNN), logistic regression (LR), and decision trees (DTs), whereas regression is represented by multilayer perceptrons (MLPs) and ensemble techniques incorporate rand forest

TABLE VIII
SUMMARY OF TYPICAL AI-BASED METHODS FOR INTERFERENCE DETECTION

Types	Learning paradigm	Techniques	Methods	Deployability	Robustness	Dataset limitations	Failure modes	References
Jamming	Supervised Learning	Classification	SVM, KNN, LR, DT, NB	★★★	▲▲▲▲	■■■■	●●❍	[119], [120], [121], [122]
		Regression	MLP	★★★	▲▲▲▲△	■■□	●●●●	[120]
		Ensemble Learning	Random forest, XGBoost	★★★☆	▲▲▲▲▲	■■■□	●●❍	[120], [121], [123]
	Deep Learning	CNNs	ResNet50, VGG16, TSFANnet, AlexNet	★★☆	▲▲▲▲	■■■■	●●❍	[124], [125], [171], [172]
		RNNs	LSTM, BILSTM	★★	▲▲▲▲△	■■■■□	●●●	[173]
		Transformer	TCN-Transformer	★★	▲▲▲▲▲	■■■■■	●●	[174]
Spoofing	Supervised Learning	Classification	KNN, LR, DT, SVM, NB	★★★★☆	▲▲▲	■■□	●●❍	[153], [175]
		Regression	MLP	★★	▲▲△	■■❍	●●❍	[153]
		Ensemble Learning	Random forest, XGBoost	★☆	▲▲△	■■■■	●●	[153], [155]
	Unsupervised Learning	Clustering	K-means	★★☆	▲△	■■□	●●●●	[154]
		Dimensionality Reduction	PCA, Autoencoder	★★★★☆	▲▲▲△	■■■	●●	[154], [176]
	Semi-supervised Learning		GANomaly network	★★★☆	▲▲▲△	■■□	●●❍	[177]
	Deep Learning	CNNs	PCA-CNNs, AdaBoost-CNN	★★★★☆	▲▲▲▲△	■■■	●●	[159], [178]
		RNNs	LSTM, PCA-CNN-LSTM	★★	▲▲▲△	■■■□	●●❍	[158], [160]
		GAN		★★★☆	▲▲▲▲	■■■■□	●●●❍	[157]

Notes:
a) Deployability: ★ - poor, ★★☆ - moderate, ★★★★★ - excellent
b) Robustness: ▲ - poor, ▲▲△ - moderate, ▲▲▲▲▲ - excellent
c) Dataset limitations: ■ - little impact, ■■❑ - moderate impact, ■■■■■ - serious impact
d) Failure modes: ● - low sensitivity to model errors, ●●❍ - moderate sensitivity, ●●●●● - high sensitivity

(RF) and extreme gradient boosting (XGBoost). Inputs are typically time-domain, frequency-domain, or measurement-level features. Figure. 6 illustrates standard SVM-based jamming detection and classification results. Alkhatib et al. [120] employed these supervised methods to identify barrage, single-tone, successive-pulse, and protocol-aware jamming. An MLP demonstrated optimal performance, achieving 98.9% detection accuracy (DA) and a 0.28% false alarm rate (FAR).

For supervised learning, feature selection is a critical factor in determining model efficacy. Common inputs include temporal, spectral, and signal-domain characteristics. The use of many features increases computational complexity during feature extraction; thus, dimensionality reduction is often applied. Qin et al. [119] optimized selection by prioritizing features correlated with jamming attributes. Alternatively, Morales et al. [122] employed SVM-based feature clustering to preprocess inputs for subsequent learning.

To reduce computational latency, direct extraction of statistical signal features (e.g., signal energy, kurtosis and entropy) can be employed. Merwe et al. [121] utilized DT and XGBoost for classifying these features. This approach achieves rapid training convergence while balancing human and ML efforts, making it suitable for SWAP-constrained platforms. Alternatively, hybrid approaches integrating conventional detection methods can be adopted. Sormayli et al. [123] implemented a sliding-window predetection mechanism for jamming-induced AGC and noise-level anomalies. It achieved 99.97% DA and 99.94% precision in cases with Ublox-M8T GNSS receivers, with a per-sample processing time of 20 μs.

b) Deep learning (DL): DL models enable automated feature extraction, surpassing the performance of traditional ML approaches. Prevalent architectures include convolutional neural networks (CNNs), recurrent neural networks (RNNs), and Transformers. These methods leverage hierarchical neural networks to extract discriminative features from 2-dimensional signal representations or 1-dimensional sequential data (e.g., power spectrum distributions and time-frequency representations).

CNNs demonstrate excellent feature extraction and classification capabilities for image-based representations, with residual networks (ResNet) and VGG networks being prominent examples. Hybrid architectures combining ResNet50's deep residual learning with VGG16's robust feature extraction exhibit exceptional recognition performance [171]. This method achieved enhanced detection rates and F1 scores for signal spectrograms, time-frequency distributions, and IQ constellation diagrams. With respect to sequential signal processing, RNNs outperform other methods in capturing long-range temporal dependencies, particularly long short-term memory (LSTM) variants [173].

The recent integration of attention mechanisms in Transformer networks has revolutionized multidimensional feature extraction through global dependency modeling. To address the substantial training data requirements for UAV-based implementations, distributed systems employing temporal convolutional network-Transformer (TCN-Transformer) architectures were proposed [174]. This framework synergized local feature extraction via TCN's historical signal analysis with Transformer's global pattern recognition. Moreover, federated learning enables efficient weight aggregation across drone clusters. It achieved 91.97% DA and a 91% F1 score, significantly reducing centralized training burdens with minimal performance degradation.

The feature extraction capability of DL models fundamentally depends on the characteristics of the input data. Common representations include power spectrum distributions (PSDs), spectrograms, histograms, STFTs, WVDs, wavelet transforms, Hilbert-Huang transforms (HHTs), and I/Q constellations [171]. While WVD and STFT enable real-time TFR generation from RF front-end data streams, practical implementation faces performance degradation issues because of hardware limitations, such as those related to quantization bit depth and filtering effects [124]. Notably, STFT efficacy varies with interference power levels. Chen et al. [125] proposed a hybrid approach combining time-frequency and time-power analysis as RF fingerprint features, achieving 95% DA with superior generalization capability, particularly for low-power interference scenarios.

The extracted signal features are often associated with challenges such as high dimensionality and redundancy. To address these issues, Reda et al. [173] developed a feature selection algorithm integrating principal component analysis (PCA) with Bayesian optimization. It achieved 98.08% DA with 97.84% F1 scores, while reducing the feature dimension by 33% and training time by 23%. Alternatively, Zhong et al. [172] proposed a temporal-spatial feature aggregation network (TSFANet) with multilevel feature fusion modules for multiscale feature extraction. Compared with CNNs and transformers (typically > 150 MB parameters), TSFANet demonstrates superior memory efficiency (3.9 MB parameters) while maintaining competitive performance.

As shown in Table VIII, in terms of real-world deployability, classic tools such as SVMs and KNNs are superior because of their low complexity, making them suitable for resource-constrained systems [119], [121]. Conversely, deep learning models, especially CNNs and RNNs, face significant deployment challenges because of their high computational and memory demands [171]. However, this is offset by their superior robustness, i.e., deep learning architectures consistently achieve higher ratings in dynamic environments because of their powerful feature extraction capabilities [125]. A major common limitation is their sensitivity to dataset quality and diversity, with all methods showing moderate to high dependency. This data-hungry nature is particularly pronounced for deep learning [172]. With respect to failure modes, traditional models may fail with complex, nonlinear interference patterns, whereas deep learning models are more likely to degrade data that differ significantly from their training distribution or in extreme signal conditions [174].

Overall, the AI-based jamming detection methods differ fundamentally in their approach to feature representation, leading to distinct performance-resource trade-offs. Traditional ML methods rely on manually engineered features (e.g., statistical moments and spectral parameters), which require significant domain expertise for feature selection and parameter dimensionality reduction. The core advantage of these methods are their relatively low computational complexity and rapid inference, making them suitable for real-time, SWAP-constrained platforms. However, their performance is inherently bounded by the quality and comprehensiveness of the manually selected features. In contrast, DL models (e.g., CNNs and transformers) perform automatic, hierarchical feature extraction directly from raw or minimally processed data (e.g., spectrograms and IQ samples). This enables superior generalization and detection accuracy for complex, unseen interference patterns. This capability comes at the cost of substantially higher computational demands for training and inference, extensive data requirements, and high model complexity, posing challenges for on-device deployment. Thus, the selection between ML and DL involves a critical balance between deployment pragmatism and analytical power, dictated by the available platform resources, data accessibility, and required level of sophistication of the detection scheme.

B. Spoofing Detection and Identification

Spoofing is detected by exploiting subtle differences between authentic and counterfeit signals. Typical detection methods are summarized in Table VII. Specific discussions of the main methods are as follows.

1) Signal Processing-Based Methods: Signal processing methods monitor signal quality changes in the receive channel and measurement anomalies caused by spoofing.

a) Signal quality monitoring (SQM): The SQM is a common navigation interference monitoring method. It evaluates signal integrity by monitoring key parameters such as amplitude, frequency, code phase, and correlation peak during signal reception and processing [127]. A typical SQM method always identifies distortions in the autocorrelation function (ACF), as defined in Eq. (8).

$$R_x(\tau) = \frac{1}{N}\sum_{n=0}^{N-1} x[n]\, x^*[n-\tau], \tag{8a}$$

$$\Delta = \max_{\tau\in[-\tau_{\max},\tau_{\max}]} \left|R_x(\tau) - R_x(-\tau)\right|, \tag{8b}$$

$$\gamma = \frac{R_x(0) - R_x(\tau_{\text{th}})}{R_x(0)}, \tag{8c}$$

$$\text{Decision} = \begin{cases} \text{Authentic}, & \text{if } \Delta < \theta_1 \text{ and } \gamma < \theta_2, \\ \text{Spoofed}, & \text{otherwise.} \end{cases} \tag{8d}$$

Here, $x[n]$ represents the discrete-time signal samples, $x^*[n]$ is its complex conjugate, τ is the time delay of the samples, and N is the window length. $\tau_{\max}$ represents the maximum detection delay, and Δ is the symmetry deviation metric. $R_x(0)$ is the zero-delay autocorrelation peak, and τ_{th} is a delay threshold. γ is the peak attenuation ratio, and θ_1, θ_2 are empirical decision thresholds.

SQMs based on ACFs suffer from strong spoofing, phase shift, and multipath issues, leading to a high FAR [128]. To address these limitations, Wang et al. [129] proposed a four-complex-correlator metric based on the quadra-phase correlation outputs. This method outperforms other methods, especially for high spoofing-signal ratios. Zhou et al. [179] leveraged the Kolmogorov-Smirnov test to detect slight distortions in different power levels in the correlation function. This method can achieve a detection rate of more than 95% at a 10% FAR while reducing alarm time and computational complexity. Zhang et al. [130] combined signal power analysis with early, punctual, and late code correlation outputs to smooth detection values. They validated the method's effectiveness based on real BeiDou spoofing data (e.g., matched-power, overpowered, static, and dynamic spoofing).

Fang et al. [128] introduced a new ACF similarity measure combined with image feature extraction to detect ACF and power distortions in tracking loops, achieving an 87% DA for the Texas Spoofing Test Battery (TEXBAT) dataset at a 1% FAR but still being affected by multipath effects. To eliminate multipath effects, Sun et al. [131] proposed a new SQM metric focusing on abnormal energy in the quadrature signal branch and developed an intersatellite cross-detection scheme to separate multipath signals from spoofing signals. This method achieved a 95% DA in TEXBAT Scenario 2 with a 1% FAR.

b) Signal feature extraction: Spoofing alters signal statistics such as power and Doppler shift. These indicators can be used as detection metrics. Key features are listed in Table IX. Since spoofing signals typically have greater power than authentic signals do and can take over tracking loop control [81], simultaneous monitoring of AGC and C/N_0 is effective. A change in AGC without a corresponding change in C/N_0 suggests spoofing, whereas a decrease in both indicates likely jamming [136]. Combining these metrics into a receiver power monitoring (RPM) framework enables adaptive threshold setting across flight phases [135].

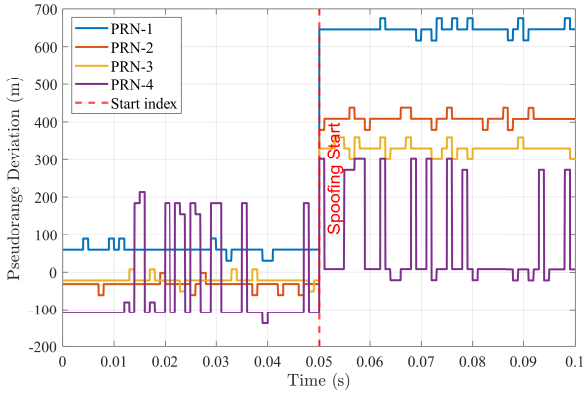
For multifeature spoofing detection frameworks, Li et al. [132] incorporated seven features, such as C/N_0 and pseudorange residuals from signal processing, observation, and solution layers. This method, combined with correlation coefficients, improved detection performance by 25% over traditional methods (e.g., clock difference detection). Wei et al. [133] introduced SigFeaDet, in which signal C/N_0 and Doppler features are used for spoofing detection. Validated via UAV experiments, it achieved over 95% DA at a 5% FAR across different UAV speeds, heights, and positions. Additionally, smoothing the C/N_0 in both in-phase and quadrature branches was effective for detecting sudden noise changes caused by spoofing signals [134]. When the spoofing signal was 5 dB stronger than the authentic signal, this improved method yielded 98% DA and a 10% FAR, whereas the traditional method yielded a 30% FAR.

TABLE IX
SUMMARY OF TYPICAL FEATURES FOR SPOOFING DETECTION

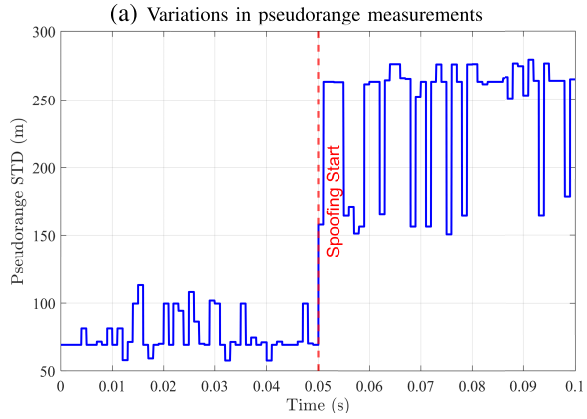
Features	Expression	Characterisics
Moving Average (MA)	$\text{MA}_t = \frac{1}{N} \cdot \sum_{i=t-N+1}^{t} x_i$	It describes short-term changes and is sensitive to sudden power fluctuations.
Moving Variance (MV)	$\text{MV}_t = \frac{1}{N} \cdot \sum_{i=t-N+1}^{t} (x_i - \text{MA}_t)^2$	It describes signal stability, and its peaks represent distortion caused by interference.
Early-Late Phase (ELP)	$\text{ELP} = \lvert E - L \rvert$ or $\sqrt{E^2 - L^2}$	It detects the offset of code phase and requires optimization of the spacing between correlators.
CNR (C/N_0)	$C/N_0 = 10 \log_{10} \left(\frac{P_{\text{signal}}}{P_{\text{noise}}} \right)$	As a direct quality indicator, the abnormal changes in C/N_0 reflect the presence of interference.
Doppler Shift	$f_d = \frac{1}{2\pi} \frac{d\phi}{dt}$ or $f_d = f_r - f_0$	It reflects changes in speed, and its inconsistency can reflect the presence of deceptive signals.
Receiver Clock Drift Rate	$\delta_{\text{clock}} = \frac{d(\Delta t)}{dt}$	Spoofing introduces abnormal clock dynamics; threshold depends on oscillator stability.
Subspace Energy Ratio	$\eta = \frac{\lVert \boldsymbol{U}_{\text{noise}} \rVert_F^2}{\lVert \boldsymbol{U}_{\text{signal}} \rVert_F^2}$	Eigen-decomposition separates spoofing signals; It reflects the components of deception signals.
Cross-Correlation Power	$\rho_{xy} = \frac{\sum_{k=1}^{K} x_k y_k^*}{\sqrt{\sum_{k=1}^{K} \lvert x_k \rvert^2 \sum_{k=1}^{K} \lvert y_k \rvert^2}}$	It reflects signal correlation and can detect synchronous deception. .

Symbol Explanation:
N: Window size for averaging
E, L: Early and late correlator outputs
P_{noise}: Power of noise/spoofing components
f_0: Nominal carrier frequency
K: Number of samples in correlation window
x_i: Signal value at time i
P_{signal}: Power of the authentic signal
f_r: Received signal frequency
$\boldsymbol{U}_{\text{noise}}$: Noise subspace eigenvector matrix

c) Radio frequency fingerprint (RFF): The RFF approach identifies spoofing by exploiting the unique characteristics of the received signal [137]. Time-frequency transforms such as wavelet or STF transforms are typically used to extract hidden signal fingerprints and leverage machine learning for signal recognition [138]. Guo et al. [139] proposed two RFF-deep learning integration methods: one preprocesses signal IQ channels for CNN input, and the other combines STFT with ResNet50 for efficient



(a) Variations in pseudorange measurements



(b) Variations in pseudorange standard deviation

Fig. 7. Monitoring of pseudorange variations for spoofing detection using multisatellite measurements.

classification. A convolutional autoencoder can also be used for adaptive threshold decision-making to increase detection rates in complex spoofing scenarios [140]. RFF can be applied both before and after correlation detection. Postcorrelation detection is less effective because of filtering-induced distortion. Challenges include high precorrelation computational cost and reduced detection reliability at low SNRs, whereas postcorrelation methods require a C/N_0 above 45 dB $\cdot$ Hz [141].

d) Measurement monitoring: Spoofing can be detected by monitoring anomalies in measurements (e.g., pseudorange, carrier phase, and clock differences). Figure. 7 shows how the pseudorange standard deviation varies across satellites, revealing spoofing when satellites are affected unequally. By comparing the pseudorange double differences between two receivers with the expected estimate, spoofing signals from different sources can be identified [142]. Shang et al. [144] examined the pseudorange difference across epochs and used a robust extended Kalman filter to reduce errors in multiple correlation measurements.

The norm of the difference between baseline vectors obtained from multiple receivers can also be used for detection [145]. By simultaneously tracking the GNSS and spoofing signals with multiple receivers and generating baseline vectors from the double-difference carrier phase measurements, the initial detection time is greatly reduced.

Spoofing signals often fail to synchronize with authentic signals because of differing propagation delays. Building on this, the quasisynchronous spoofing localization method exploits time difference measurements to estimate the difference in distance between the spoofer and receiver [143]. Truong et al. [146] detected spoofing by monitoring the deviations of clock bias after switching from an authentic to a spoofing signal. Monitoring clock bias is a low-cost and effective approach, especially for GNSS-reliant UAVs.

In summary, this subsection describes four signal processing-based spoofing detection strategies, each operating at a distinct layer of the receiver chain and exploiting different artifacts introduced by a spoofer. The SQM scrutinizes distortions at the correlation level (e.g., in the autocorrelation function), offering direct sensitivity to signal overlap but facing a fundamental trade-off with multipath interference. Signal feature extraction leverages anomalies in readily available observable parameters (e.g., C/N_0 and Doppler shift), enabling low-complexity, multimetric fusion at the cost of potential confusion with natural signal dynamics. The RFF targets unique, physical-layer transmitter imperfections from the raw signal, providing high specificity against advanced spoofing at the expense of significant computational overhead and data quality requirements. Finally, measurement monitoring includes consistency checks at the navigation solution level (e.g., pseudorange, clock bias), offering a low-incremental-cost approach whose effectiveness involves a trade-off with detection latency or the need for additional hardware (e.g., multiple receivers).

A comparative analysis reveals a clear spectrum of trade-offs, primarily involving analytical depth, implementation cost, and environmental robustness. SQM and RFF constitute deep-inspection methods that probe the signal's fundamental properties, yielding high detection specificity but demanding considerable processing resources and exhibiting sensitivity to channel impairments such as noise and multipath effects. In contrast, feature extraction and measurement monitoring are pragmatic, system-integrated methods that utilize existing receiver outputs or states, resulting in low complexity and easy deployment. However, they compensate with high false alarm susceptibility to benign dynamics or require spatial hardware diversity for timely alerts. Consequently, the selection hinges on a critical balance between the required level of spoofing discrimination and the constraints imposed by platform resources and the operational electromagnetic environment.

2) Array Antenna-Based Method: The array antennas estimate the DOA of all incoming signals, including spoofing signals. By identifying discrepancies in the DOA, spoofing signals can be detected, and the direction of the spoofer can be estimated. Esswein et al. [148] exploited the polarization differences between authentic and spoofing signals to distinguish multiple spoofers. Differences in carrier phase across antennas also enable spoofing detection and spoofer localization via multireceiver observations [149].

The number of degrees of freedom (DOFs) of array antennas influences the ability of these arrays to handle spatial interference. DOFs are limited by the number of antenna elements; i.e., arrays can only handle signals lower than the element count. Increasing the number of elements increases the hardware cost and thus restricts the application of

resource-constrained UAVs. To address this problem with a fixed number of elements, Zhao et al. [150] used coprime arrays to enhance processing flexibility. By constructing a noise-reduction covariance matrix and applying DOF-enhancement decorrelation, this method effectively detected spoofing even when the signal count exceeded the element count. To reduce hardware resource consumption, Chen et al. [151] proposed a spoofing detection scheme with three low-cost colinear antennas. Via the use of antenna colinearity-constrained observation equations, this approach improved direction-vector estimation precision, reducing the pointing-angle error standard deviation by 55% and enabling real-time spoofing detection. Furthermore, the sum-of-square-error (SSE) method combines baseline priors with carrier-phase differences to detect single- or multidirectional spoofing in real time, even when only a few array elements are available [152].

Overall, the array-based spoofing detection methods discussed above address the trade-off between spatial discrimination capability and hardware feasibility, governed by DOF limitations. Conventional DOA estimation techniques face a hard performance ceiling based on the number of antenna elements. Subsequent innovations diverge along two paths. One path involves employing advanced algorithmic processing steps, such as coprime arrays and enhanced decorrelation, to overcome the DOF limit. This approach improves robustness against multiple spoofers while leading to higher computational cost. The other path involves adopting a minimalist hardware design. Low-cost collinear arrays or geometric constraints are used to achieve practical and real-time detection suitable for resource-constrained platforms. These paths highlight the core design compromise: extending performance through sophisticated algorithms versus ensuring deployability through streamlined hardware and efficient processing.

3) Artificial Intelligence-Based Methods: Spoofing signals exhibit minimal distinguishable features in power spectrograms and time-frequency representations because of their structural similarity with authentic GNSS signals. Consequently, AI-based detection primarily occurs at the post-correlation stage, leveraging signal observables and derived measurement parameters for spoofing identification. Representative methodologies are categorized in Table VIII.

a) Machine learning: Unlike jamming detection, spoofing detection benefits from both supervised and unsupervised learning approaches. Aissou et al. [155] conducted a comprehensive comparison of tree-based machine learning methods (e.g., RF, XGBoost, and LightGBM). They reported that XGBoost is particularly suitable for UAV applications because of its superior performance, with 95.25% DA, 4.3% FAR, and 2 ms processing latency. Unsupervised methods such as K-means with PCA or autoencoders avoid the need for labeled spoofing data. Khoei et al. [154] systematically evaluated both paradigms and reported the exceptional feature extraction ability of an autoencoder (e.g., C/N0, pseudorange, and correlator outputs), with 99.53% DA, a 1% FAR, and a 0.39 s inference time.

Fusing SQM metrics with observables such as the CNR, Doppler shift, and pseudorange enables multidomain detection. This approach combines observation-domain, signal-domain, and computational-domain characteristics. Specifically, two-dimensional correlation functions and one-dimensional features can be processed in parallel by dual-branch networks [177]. Sefercik et al. [176] proposed a temporal-spatiovariational autoencoder (TSVAE) that reconstructs signals on the basis of spatiotemporal features. By employing clean GNSS signals as attention mechanism inputs, this method enhances traditional SQM by expanding feature dimensions, and composite detection metrics from in-phase and quadrature components are constructed, achieving 99.1% DA and 99.5% F1 scores.

Detection performance can be further enhanced by incorporating navigation solution data, such as real-time GPS measurements and UAV state parameters during flight operations. Nayfeh et al. [153] validated this approach using actual flight datasets and logistic regression. They demonstrated effective detection of both static and dynamic spoofing with low computational overhead (i.e., 96.77% precision, 1.59% FAR, and 0.22 ms latency). Their method capitalized on multisensor consistency verification, where GNSS-derived position and velocity data are cross-validated with inertial measurements (e.g., gyroscope attitude) to construct robust feature sets [175].

b) Deep learning: DL effectively captures the nonlinear correlations among spoofing-induced feature distortions. Notably, spoofing introduces systematic anomalies in the ACF. Thus, Mao et al. [158] employed LSTM to analyze ACF distortions. Their approach detected diverse spoofing types (e.g., power disparities and code and phase offsets) with a 98.5% detection rate at a 5 ms latency.

When spoofing deviates only slightly from authentic signals, single-peak acquisition patterns occur. Li et al. [157] used GAN-based discriminators to amplify subtle signal discrepancies, achieving a more than 98% detection rate when the code phase difference exceeds 0.5 chips. Iqbal et al. [180] further used a variational autoencoder (VAE) and a GAN. The features used for training are extracted from the radio frequency and tracking modules of a standard GNSS receiver. When tested on the TEXBAT dataset, the detection performance across simple to intermediate datasets for the proposed detectors reaches approximately 99%, demonstrating high robustness. For UAV-specific scenarios with limited training data, She et al. [178] developed an AdaBoost-CNN framework that combines multiple weak CNNs into a robust classifier via parameter transfer learning. This approach achieved 95.83% accuracy with only 120 measured samples and precisely identified spoofing types (e.g., static/dynamic, position/time, and power-matched/overpowered).

To address model compression and data scarcity issue, researchers have developed hybrid approaches that integrate dimensionality reduction with deep learning. Korium et al. [159] pioneered a CNN-PCA framework that transformed extracted features into composite images coupled with transfer learning to enhance generalization. This approach achieved 99.25% DA with 2.72 s latency and significantly expanded effective training diversity. For temporal signal analysis, Sun et al. [160] proposed a PCA-CNN-LSTM cascade model.

TABLE X
SUMMARY OF TYPICAL GNSS INTERFERENCE DATASETS

Types	Name	Content	Reference
Jamming	GNSS processed interference features	Spectral features of 72 million randomly generated interference signals (e.g., single-tone, multi-tone, linear chirp, and band-limited noise).	[181]
	Multi-feature GNSS jamming (MFGJ)	Spectrum images of eleven types of interference and navigation signals (e.g., chirp, CWI, pulse, spread spectrum jamming).	[172]
	Public GNSS jamming	Feature images of the clean signal and five types of jamming signals (e.g., amplitude modulated jamming, FM jamming, narrowband jamming).	[122]
Spoofing	Texas Spoofing Test Battery (TEXBAT)	Features of fixed synchronous and asynchronous spoofing (e.g., receiver clock bias, C/N_0, doppler frequency offset).	[182]
	Oak Ridge Spoofing and Interference Test Battery (OAKBAT)	More test scenarios for spoofing research compared to TEXBAT (e.g., GPS and Galileo spoofing).	[183]
	UAV attack dataset	Flight datasets under normal flight and interference, including simulation and actual testing.	[184]

The PCA first condenses the GNSS data dimensionality; then, the CNN extracts spatial features from the reduced data, and the LSTM captures the temporal dependencies. This method achieved 99.43% DA and a 97.22% F1-score for composite-wing UAVs.

Artificial intelligence approaches, encompassing both traditional machine learning and deep neural networks, are fundamentally data-driven modeling methods. The performance of trained models critically depends on the quantity and quality of datasets, as exemplified by the existing GNSS interference datasets in Table X. The current benchmark datasets primarily consist of interference signals and their extracted features but exhibit notable limitations in addressing emerging complex interference scenarios.

As shown in Table VIII, a clear evaluation between deployability and robustness across AI methods for spoofing detection is presented. Traditional supervised learning methods (e.g., KNN, SVM, and decision trees) offer the highest deployability because of their low computational complexity, making them suitable for resource-constrained systems [153]. In contrast, deep and semisupervised learning models (e.g., CNNs and GANomaly) achieve superior robustness against dynamic and novel attacks but present significant deployment challenges owing to high computational demands [159]. Furthermore, deep learning models rely strongly on large-scale and high-quality training data; thus, their primary failure risk stems from performance degradation under data distribution shifts [158]. Traditional and unsupervised models with comparatively less data reliance face inherent algorithmic limitations, such as an inability to model highly nonlinear decision boundaries or sensitivity to poor feature engineering [154], [177]. Ensemble methods can mitigate some single-model failures but may fail if base learners are highly correlated [155].

In summary, the AI-based spoofing detection methods discussed herein fundamentally diverge into two paradigms with distinct data-processing philosophies and inherent performance-resource trade-offs. The ML paradigm primarily operates on the basis of the features of signal processing-based methods, leveraging both supervised and unsupervised models. This approach offers the advantages of relatively low computational complexity and fast inference times, making it suitable for real-time UAV applications. However, its effectiveness is intrinsically bounded by the quality of the engineered features. In contrast, the DL paradigm employs end-to-end hierarchical models to automatically extract complex and nonlinear patterns from raw or minimally processed inputs. This enables superior capability in capturing subtle and systematic anomalies and generalizing to complex spoofing types. This enhanced performance comes at the cost of significantly higher computational demand and model complexity and a notable reliance on large, high-quality training datasets.

This reveals a core trade-off between model sophistication and practical deployment constraints. ML methods excel in scenarios with limited data, but their detection accuracy may have a potential upper limit when dealing with novel or highly complex spoofing attacks. DL methods push the boundaries of detection performance and feature discovery but face challenges in terms of computational load and data reliance. To mitigate the data dependence of DL methods, recent hybrid approaches (e.g., AdaBoost-CNN and PCA-CNN-LSTM) integrating dimensionality reduction and transfer learning have been developed, effectively bridging the gap by enhancing generalization with limited samples. Therefore, the selection between ML and DL methods for UAV spoofing detection is not merely algorithmic but strategic, depending on the available onboard computational resources, the accessibility and quality of training data, and the required level of sophistication of the detection scheme against evolving threats.

4) System-Aided Detection: Inertial navigation and vision systems, which are unaffected by GNSS interference, can assist in detecting interference, particularly erroneous measurements caused by spoofing.

a) INS-aided detection: Owing to their resistance to external electromagnetic interference, INSs are an ideal choice for spoofing detection [163]. Feng et al. [161] compared the angular velocity integral of gyroscopes with GNSS-measured heading changes. On the basis of the sensitivity to the angular and velocity changes of INSs, this approach was effective for low-complexity spoofing detection for quadcopters on both straight and curved flights. Feng et al. [162] proposed a two-step training method based on GA-XGBoost with both historical and real-time sensor data. Applying the GA to optimize XGBoost parameters enabled successful spoofing attack detection within 1 second of onset.

b) Communication-aided detection: The UAV-to-ground communication link remains unaffected by GNSS spoofing and can be exploited for detection. This is especially true with the large-scale deployment of 5G base stations and the widespread use of UAV formations [164]. 5G networks can deliver

auxiliary data (e.g., satellite ephemeris, approximate position, and time) to GNSS receivers. Time difference of arrival (TDOA)-based coarse positioning can be achieved through 5G signals. Moreover, hybrid 5G-GNSS integration enables joint high-precision positioning. Bai et al. [165] proposed a three-level true position estimation algorithm. It uses extended Kalman filtering to fuse GNSS and 5G signal measurements, performing coarse estimation, fine estimation, and true signal restoration in sequence. Dang et al. [166] mapped the trajectory offset of UAVs caused by GNSS spoofing to the propagation loss of the communication path. By analyzing path loss decisions, a 97% spoofing detection rate is achieved with two receiving base stations.

c) Image-Aided detection: Visual sensors on UAVs can detect spoofing by comparing visual odometry with GNSS positions. For instance, video streams often include associated GPS coordinates; comparing these with calculated positions helps identify positional deviations of approximately 2.5 meters [167]. Wang et al. [168] extracted ORB features from monocular camera streams and estimated attitude via homography transformation. By fusing these visual attitude angles with IMU data and comparing them against GNSS outputs, they detected spoofing-induced anomalies in latitude, longitude, and altitude, achieving a 98.75% detection rate within an average of less than 1 second. Leveraging visual sensors for spoofing detection during environmental perception offers a cost-effective, real-time solution, though its performance depends on stable environmental features such as adequate lighting and flight altitude [169].

In summary, the system-aided spoofing detection methods surveyed here leverage external or independent sensor data to cross-validate GNSS-derived information, exploiting inconsistencies introduced by spoofing. The three subcategories, INS-aided, communication-aided, and image-aided detection, rely on distinct reference sources and principles. INS-aided methods use inertial sensors, which are immune to RF interference, to check consistency between IMU data and GNSS dynamics. This approach is low-complexity and autonomous but faces a trade-off between detection accuracy and the accumulating drift of low-cost MEMS-INS. Communication-aided methods, especially with 5G, establish an external RF reference via the unspoofed UAV–ground link, using techniques such as TDOA-based positioning or fused 5G–GNSS filtering to detect anomalies. These introduce dependence on network coverage and availability. Image-aided methods provide a passive environmental reference by comparing visual odometry or geotagged video with GNSS positions. While cost-effective and dual-purpose, their effectiveness is constrained by environmental conditions and flight altitude.

A comparative analysis reveals a spectrum of trade-offs centered on autonomy, environmental dependence, and system integration complexity. INS-aided detection provides complete autonomy and a fast response but is ultimately bounded by sensor quality and drift. Communication-aided methods offer high accuracy and infrastructure-level validation but sacrifice operational independence and geographical freedom. The image-aided method strikes a different balance when onboard cameras are used for passive and feature-based environmental referencing but requires sufficient and stable visual features to operate reliably. Consequently, the choice among these submethods involves a strategic decision based on the operational environment (e.g., urban or remote), available infrastructure for 5G coverage, mission duration, and platform capabilities (e.g., camera and processing power), with a trend toward hybrid solutions that combine their complementary strengths for resilient UAV navigation.

C. Performance Evaluation and Selection Guidelines

To provide concrete guidance for selecting interference countermeasures, a unified evaluation framework based on four critical metrics is established: detection accuracy, false alarm rate, computational load, and deployment readiness (e.g., hardware requirements). A consolidated summary of these metrics for all the reviewed methods is presented in Table IX. The following subsections offer a synthesized, cross-method analysis of detection techniques to jamming and spoofing, concluding with actionable selection advice tailored to different UAV operational scenarios.

1) Techniques for Jamming:

a) Cross-Method comparative analysis: The analysis of jamming detection methods, as summarized in Table IX, reveals clear trade-offs between analytical performance and resource consumption. AI-based methods, particularly deep learning methods, achieve the highest detection accuracy when complex spectral-temporal features are learned. However, this comes at the cost of a high computational load and a dependence on extensive training data. Array antenna-based methods provide high accuracy and unique spatial filtering capabilities but are characterized by a triangular trade-off involving performance, hardware cost, and computational load for direction-finding algorithms.

In contrast, conventional signal processing methods prioritize practicality. They exhibit low-to-moderate computational load and minimal hardware needs. Their main trade-off is between efficiency and robustness: while TF analysis offers good accuracy, it is computationally more intensive than AGC. The AGC detector is extremely lightweight but is characterized by low accuracy and high susceptibility to false alarms from legitimate signal power variations.

b) Selection advice for UAV platforms: On the basis of the aforementioned analysis, the optimal choice of method depends on the constraints of platform SWaP consumption and cost. For medium-sized commercial and tactical UAVs with sufficient payload and processing capabilities, high-performance solutions can be utilized. For instance, array processing based on a limited number of antennas is highly suitable for robust interference detection. Furthermore, when adequate training data and on-board computational resources are available for inference, deep learning methods can be employed to achieve superior detection accuracy for complex or evolving interference patterns.

For small consumer UAVs with strict SWaP constraints, the balance between performance and resource consumption is crucial. Techniques involving AGC detectors or lightweight feature monitoring offer a default and low-cost solution. When data for specific scenarios are available, the use of lightweight

machine learning models is a favorable compromise that provides higher accuracy than traditional methods with a controllable increase in computational load.

2) Techniques for Spoofing:

a) Cross-Method comparative analysis: Spoofing detection methods exhibit broad diversity in terms of their operating principles and associated trade-offs, as shown in Table IX. AI-based methods yield high accuracy, with DL outperforming traditional ML. The trade-off remains significant in terms of computational cost and data dependence. Signal processing methods diverge on the basis of their inspection layer: SQM provide good accuracy but high false alarm rates in multipath cases and trade sensitivity for environmental robustness. RFFs provide high specificity by exploiting physical-layer features but at high computational and hardware costs.

For simplicity, measurement-based methods are low cost but slower than other methods, trading timeliness for simplicity. Array-based methods for spoofing share similar trade-offs as those for jamming: high-accuracy spatial discrimination versus hardware complexity and computational load. System-aided methods introduce a different paradigm, trading platform autonomy for external integrity verification. Their accuracy is often moderate, but they add a valuable independent check, with deployment feasibility being a key constraint.

b) Selection advice for UAV platforms: With the support of various current deception detection methods, the selection process must consider the deception threat model and operational environment. For medium UAVs, these platforms can implement multilayer defense. For example, combining DL-based signal analysis with system-aided checks (e.g., INS and visual) creates a robust, hybrid solution that mitigates the weaknesses of individual methods, leveraging the available payload for diverse sensors.

For small UAVs, the focus is on efficient, receiver-integrated technologies. Lightweight machine learning models trained on key features (such as C/N_0 and pseudorange information) provide a good balance. Moreover, basic measurement consistency checks add minimal overhead. Although system-aided detection is challenging because of the need for auxiliary sensors, low-cost MEMS-IMUs can be valuable resources for consistency monitoring.

In summary, this evaluation demonstrates that no single method dominates across all metrics. The selection framework highlights a consistent engineering compromise: advanced methods (e.g., AI-based and array-based) achieve better performance at the expense of computational and hardware resources, whereas simpler methods (e.g., conventional signal processing and lightweight ML) favor deployability under strict SWaP constraints. The optimal strategy for resilient UAV navigation often involves the intelligent hybridization of complementary techniques tailored to specific platform capabilities and mission threat profiles.

V. Interference Mitigation and Suppression

Interference mitigation aims to alleviate the degradation of navigation services or to reconstruct the GNSS signal waveform in the presence of interference [185]. Following detection, the mitigation stage involves applying countermeasures tailored to the identified interference class [186]. As summarized in Table XII, current techniques fall into three categories: signal processing, array antennas, and artificial intelligence-based algorithms.

TABLE XI
METRICS OF INTERFERENCE DETECTION AND IDENTIFICATION

Types	Specific techniques	Detection accuracy	False alarm rate	Computa -tional load	Deployment readiness
Jamming	TF analysis based	★★★☆	▲▲	■■	A
	AGC based	★★★	▲▲△	■❑	A
	Array antenna based	★★★☆	▲▲△	■■■	B
	Supervised learning	★★★★☆	▲▲	■■■❑	C
	Deep learning	★★★★★	▲△	■■■■❑	A/B
Spoofing	SQM	★★★☆	▲▲▲	■■❑	A
	Feature analysis based	★★★	▲▲▲△	■■■❑	B
	RFF	★★★★	▲▲	■■■■	C
	Measurement based	★★☆	▲▲▲△	■■❑	A/B/C
	Array antenna based	★★★☆	▲▲△	■■■❑	B
	Supervised learning	★★★★☆	▲▲△	■■■■	A/B
	Semi-supervised learning	★★★☆	▲▲▲	■■■■❑	A/B
	Deep learning	★★★★★	▲△	■■■■■	C
	INS aided	★★★	▲▲△	■■■	D
	Communication system aided	★★	▲▲△	■■■	D
	Visual system aided	★★★	▲▲	■■■■	D

Notes:
a) Detection accuracy: ★ - low ($\leq 85\%$), ★★☆ - moderate ($85\% - 95\%$), ★★★★★ - high ($\geq 95\%$)
b) False alarm rate: ▲ - low ($\leq 1\%$), ▲▲△ - moderate ($1\% - 5\%$), ▲▲▲▲▲ - high ($\geq 5\%$)
c) Computational load: ■ - low, ■■❑ - moderate, ■■■■■ - high
d) Deployment readiness: A - Single antenna, B - multi antennas, C - special receivers, D - auxiliary sensors

A. Jamming Mitigation and Suppression

Traditional mitigation techniques, such as filtering and spectral analysis, are effective against interference with known characteristics, whereas array antennas filter signals from a spatial perspective regardless of the specific characteristics. Emerging AI-based approaches offer unique advantages in handling unmodeled or adaptive interference and complex environments.

1) Signal Processing-Based Methods: Traditional signal processing involves the application of antijamming filters after the RF end to filter and remove interference from mixed signals. This approach can also leverage time-frequency analysis to concentrate interference signals for suppression.

TABLE XII
SUMMARY OF INTERFERENCE MITIGATION AND SUPPRESSION METHODS

Interference Types	Approach Categories	Specific Techniques	Operating Mechanisms	Technical Constraints	References
Jamming	Signal Processing Based	Notch filter	Attenuate and filter the frequency point of the jamming signal.	Broadband interference cannot be suppressed; Filter frequency points should be aligned with the jamming frequency.	[187], [188], [189], [190], [191], [192], [193]
		Time-frequency transform	The jamming signals are separated from the GNSS signals in the transform domain and then suppressed by filtering.	It is difficult to achieve a balance of resolution; Multiple jamming produces cross interference during transformation.	[194], [195], [196], [197], [198], [199], [200], [201], [202]
	Array Antenna Based	Array signal processing	Beamforming is achieved to support spatial filtering for the jamming direction.	Arrays consume hardware resources; Interference suppression capability is limited by the number of array elements.	[203], [204], [205], [206], [207], [208], [209], [210]
	Artificial Intelligence Based	Deep learning	The neural networks are used to separate the interference and GNSS signal by learning the signal correlation.	Complex networks increase the consumption of computing resources; Suppression performance depends heavily on training data.	[211], [212], [213], [214], [215]
Spoofing	Signal Processing Based	Multicorrelator	Multiple correlators correct the correlation peak error caused by deception, in turn reducing the measurement error.	Multiple correlators increase hardware resource consumption.	[144], [216], [217], [218]
		Measurement correction	Use the correlation of measurement values to eliminate errors caused by spoofing.	This only effectively applies to situations where different receivers are interfered with by the same deception signal.	[219], [220], [221], [222], [223], [224]
	Array Antenna Based	Array signal processing	Estimate the arrival angle of the spoofing signal, and then use beamforming to suppress the signal in that direction.	Arrays consume hardware resources; Interference suppression capability is limited by the number of array elements.	[225], [226], [227], [228], [229]
	Artificial Intelligence Based	Machine learning	The model identifies and eliminates outliers, thereby achieving measurement bias correction.	With its limited suppression capability, it is unable to correct abnormal measurements.	[230]
		Reinforcement learning	Adjust response strategies dynamically on the basis of the impact of spoofing.	The mitigation performance relies heavily on complex network models and training datasets.	[231], [232], [233], [234]
	System Integration Based	Tightly coupled GNSS/INS	Correct the bias caused by spoofing using the short-term accuracy of INSs.	High requirements for fusion filtering algorithms.	[235], [236], [237], [238]

a) Notch filter: Notch filters attenuate input signals at specific frequencies to suppress interference. Adaptive notch filters (ANFs) dynamically adjust the notch frequency through the FLL to track the jamming signal, especially for jamming at varying frequencies. As shown in Eq. (9), the typical power ratio-based strategy improves the fidelity between the received waveform and its nominal model, thus suppressing frequency jitter and enhancing subsequent acquisition and tracking [187].

ANFs are effective against narrowband interference such as CWI. However, improper notch frequency or bandwidth settings may distort GNSS signals, resulting in pseudorange measurement deviations [189] and modulation-related clock deviations [190]. These effects on the receiver are typically assessed using metrics such as peak-to-noise-floor ratio, code bias, and code jitter [188].

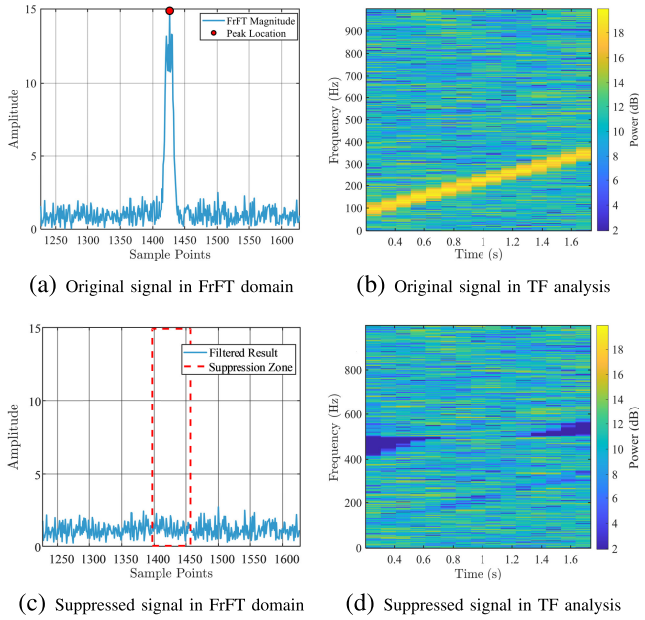
$$H(z) = 1 - w[n] \cdot z^{-1} + z^{-2}, \tag{9a}$$

$$w[n+1] = w[n] + \mu \cdot e[n] \cdot (x[n-1] + x[n+1]), \tag{9b}$$

$$\hat{f}_j[n] = \frac{1}{2\pi} \cos^{-1}\left(\frac{w[n]}{2}\right), \tag{9c}$$

$$e[n] = d[n] - y[n] = x[n] - w[n]x[n-1] + x[n-2], \tag{9d}$$

where $w[n]$ denotes the adaptive weight coefficient and z^{-1} and z^{-2} represent the unit delay operator and two-sample delay, respectively. The parameter μ $(0 < \mu < 1)$ controls



(a) Original signal in FrFT domain (b) Original signal in TF analysis

(c) Suppressed signal in FrFT domain (d) Suppressed signal in TF analysis

Fig. 8. The suppression of sweep frequency jamming based on FRFT.

the convergence rate, and $e[n]$ defines the error between the desired reference signal $d[n]$ and the filter output $y[n]$. The input signal $x[n]$ contains both GNSS signals and interference. The instantaneous jamming frequency is estimated as $\hat{f}_j[n]$, where $\cos^{-1}(\cdot)$ yields the inverse cosine in radians.

To minimize distortion, Song et al. [191] proposed adaptive sparse filtering (ASF), which dynamically adjusts filter characteristics on the basis of the interference and signal bandwidth relationship, thereby preserving signal integrity while suppressing the jammer. To enhance ANF tracking of dynamic interference, Merwe et al. [192] introduced the multiparameter adaptive notch filter (MPANF). They applied three consecutive ANFs to dynamically adjust the notch loop bandwidth, width, and depth. This method is particularly effective for suppressing rapidly changing signals such as chirp signals while reducing signal distortion. Additionally, with a check unit to monitor the changes in interference conditions, switchable iteration factors can be used to update the ANF state on the basis of detected jamming types [193].

b) Time-frequency transform: Time-frequency transforms can separate signals and interference in the time-frequency domain. By filtering out the interference and applying the inverse transform, common interference types such as narrowband, broadband, and pulse jamming interference can be suppressed [194]. When combined with techniques such as nonnegative matrix factorization (NMF) [195], time-frequency transforms can be used to precisely identify and suppress narrowband and broadband jamming within specific regions of the time-frequency plane. The fractional Fourier transform (FRFT) is typically used to suppress interference signals with time–frequency varying characteristics (e.g., sweep jamming), as demonstrated in Fig. 8. To quickly determine the optimal FRFT order, methods such as energy residual searching [197] and the first-order moment of magnitude of the FrFT approach [198] can be used. After the interference parameters from time–frequency transforms are estimated, notch filtering can be further applied for suppression [199]. The estimated parameters (e.g., chirp rate) can also be used to adjust the observations and state noise in Kalman filtering for tracking interference signal parameters [200].

Wavelet transforms decompose signals into components at different scales for multiscale analysis. Kambham et al. [196] proposed a parameterized wavelet packet thresholding method based on improved particle swarm optimization (IPSO). They adopted IPSO to determine the optimal threshold for wavelet packet decomposition and the number of layers. An adaptive threshold function based on the soft sign function was applied for flexible handling of various signal types. Additionally, the Zak transform can be applied for long-sequence signals or when fine-scale local time-frequency analysis is needed [201]. When dealing with complex multiple interference, TF transforms may encounter cross-term interference. To address this issue, Sun et al. [202] proposed a method based on the Radon–Wigner transform to effectively suppress cross-term interference.

In summary, two core signal-processing approaches for jamming mitigation are compared in this subsection. The Notch filter operates directly in the frequency domain, selectively attenuating the high-energy spectral component. It offers high computational efficiency and real-time feasibility, making it highly effective against narrowband and swept-tone jammers. However, its core weakness is the inherent trade-off between the suppression depth and signal integrity. Conversely, time–frequency transform methods operate in the joint time–frequency domain, which allows them to concentrate on and isolate the energy of nonstationary interference, such as chirp and pulsed signals. This grants them superior capability against complex jammers, but this comes at the cost of significantly higher computational complexity because of the required transformations and the need to address cross-term interference in multicomponent scenarios.

The selection between these methods thus hinges on the jammer characteristics and platform constraints. For resource-constrained UAVs facing primarily narrowband threats, enhanced ANF/MPANF offers a pragmatic, low-latency solution. For platforms with greater processing capability operating in complex electromagnetic environments, time–frequency transform-based methods provide the necessary analytical depth to excise sophisticated interference, justifying greater computational investment. A hierarchical strategy that employs a lightweight notch filter as a first line of defense with selective activation of a more sophisticated time-frequency processor can optimally balance this performance-resource trade-off.

2) Array Antenna-Based Methods: Array antennas suppress interference through beamforming, as shown in Fig. 9. By adjusting element weights to form nulls in the jamming direction, arrays effectively suppress narrowband and broadband interference. They can also suppress jamming and spoofing interference separately via subspace separation techniques [203]. Common array processing criteria include power minimization, variance minimization, and mean square error minimization [204]. These criteria have been used to establish typical algorithms such as the power inverse (PI) algorithm and

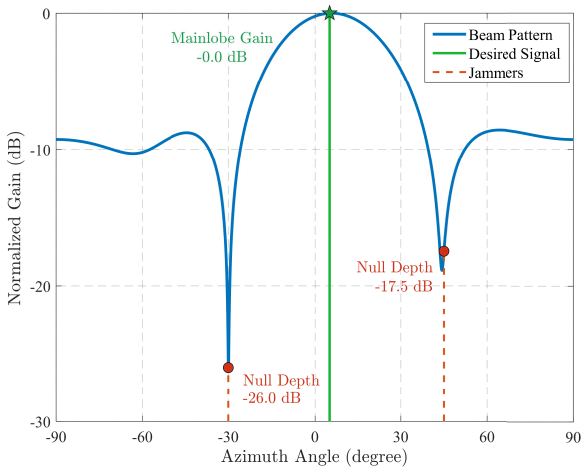


Fig. 9. Adaptive beamforming pattern for jamming suppression using a four-element array with one GNSS signal and two jamming sources (the same situation as in Fig. 5).

minimum variance distortionless response (MVDR) algorithm as follows.

- **PI** [205]: This adjusts the weighting vector to minimize the array output power, creating nulls in the direction of interference to suppress interference, as illustrated below.

$$\boldsymbol{w}_{\text{opt}} = \frac{\boldsymbol{R}^{-1}\boldsymbol{s}}{\boldsymbol{s}^H\boldsymbol{R}^{-1}\boldsymbol{s}}, \tag{10a}$$

$$P_{\text{out}} = \boldsymbol{w}^H\boldsymbol{R}\boldsymbol{w}, \tag{10b}$$

$$\boldsymbol{R} = \mathbb{E}\left[\boldsymbol{x}(t)\boldsymbol{x}^H(t)\right], \tag{10c}$$

  where $\boldsymbol{w}$ denotes the weight vector, $\boldsymbol{R}$ represents the covariance matrix of the received signal vector $\boldsymbol{x}(t)$ at time t, $\boldsymbol{s}$ is the steering vector of the desired signal, and $\mathbb{E}[\cdot]$ is the expectation operator. The Hermitian transpose $(\cdot)^H$ ensures conjugate symmetry in complex-valued signal processing.
- **MVDR** [206]: MVDR optimizes the weighting vector to minimize the output signal variance while keeping the signal from the desired direction unchanged, which is expressed as follows.

$$\min_{\boldsymbol{w}} \boldsymbol{w}^H\boldsymbol{R}\boldsymbol{w} \quad \text{subject to} \quad \boldsymbol{w}^H\boldsymbol{s} = 1, \tag{11a}$$

$$\boldsymbol{w}_{\text{MVDR}} = \frac{\boldsymbol{R}^{-1}\boldsymbol{s}}{\boldsymbol{s}^H\boldsymbol{R}^{-1}\boldsymbol{s}}, \tag{11b}$$

$$P_{\text{out}} = \boldsymbol{w}^H\boldsymbol{R}\boldsymbol{w}, \tag{11c}$$

  where $\boldsymbol{w}$ is the weight vector designed to minimize the total output power while preserving the distortionless response in the desired direction, as $\boldsymbol{w}^H\boldsymbol{s} = 1$ shows. This differs from PI, which focuses solely on nulling interference without explicit distortionless constraints.

Arrays can suppress signals from specific directions, but channel inconsistencies can cause phase center deviations, leading to errors in pseudorange and carrier-phase measurements [207]. Daneshmand et al. [208] proposed a two-stage array suppression method. First, conventional space array processing (SAP) is used to estimate the interference-free subspace and project the signal. Then, a distortionless SAP filter is designed to minimize mutual correlation and maximize the SNR. For mobile platforms such as vehicles and aircraft, distributed antennas or small subarrays can achieve equivalent array processing. However, an antenna spacing exceeding half a wavelength can cause signal delay and reduce signal correlation, affecting suppression performance. Brachvogel et al. [209] used space-time array processing (STAP) to compensate for signal delays introduced by large antenna baselines and to restore correlations. Experiments with sparse subarrays on vehicles revealed that STAP significantly enhances the CNR and positioning precision, especially under wideband interference.

In summary, array antenna-based jamming suppression relies on adaptive beamforming, with the PI and MVDR algorithms representing two core optimization methods. The PI algorithm offers computational simplicity but lacks an explicit constraint to preserve the desired signal. In contrast, the protection capability for the desired signal in the MVDR algorithm provides a more theoretically sound solution for maintaining signal fidelity. However, the performance of this approach is highly sensitive to model errors, such as steering vector mismatches caused by channel inconsistencies or antenna phase center variations.

When UAVs utilize distributed antennas to achieve equivalent array processing, their performance may degrade because of excessive antenna spacing, leading to increased latency and reduced signal correlation. STAP technology addresses this issue by jointly processing signals in both space and time. This approach compensates for delays and effectively restores correlations in sparse or distributed arrays, albeit with an increased computational cost. Therefore, the choice between PI and MVDR involves a trade-off between robustness and optimality, whereas the adoption of STAP introduces a further trade-off between suppression performance under practical constraints and system complexity.

3) Artificial Intelligence-Based Methods: AI has proven effective in interference detection and is being increasingly used in interference suppression [211]. AI-based jamming mitigation fundamentally involves separating the obscured navigation signal from interference. While supervised machine learning struggles with signal recovery, DL models have become the predominant approach, as illustrated in Table XIII. DL models autonomously extract features from signals without requiring prior knowledge of interference models or RF environmental parameters.

The direct-prediction approach leverages neural networks to learn the nonlinear characteristics of navigation signals, enabling the reconstruction of obscured GNSS signals from interference-corrupted observations. Sun et al. [213] employed a deep convolutional neural network to separate satellite signals that coexist with co-frequency interference, achieving 36 dB interference suppression and weak signal recovery without requiring precise channel parameters. Wang et al. [214] compared the performance of reservoir computing (RC), MLP, and LSTM networks in direct signal separation. The experimental results demonstrated that the inherent memory mechanism of LSTM effectively eliminates interference by learning sequential patterns, whereas RC maintains a bit error

TABLE XIII
SUMMARY OF TYPICAL AI-BASED METHODS FOR INTERFERENCE MITIGATION

Types	Learning paradigm	Techniques	Methods	Deployability	Robustness	Dataset limitations	Failure modes	References
Jamming	Supervised Learning	Regression	MLP	★★ ★	▲▲▲	■■■	●●●❍	[214]
	Deep Learning	CNNs	Multilayer CNN	★★ ☆	▲▲▲	■■■❑	●●●❍	[213], [239], [240], [241], [242]
		RNNs	Reservoir Computing, LSTM	★★ ☆	▲▲▲△	■■■■	●●●❍	[214], [215]
Spoofing	Supervised Learning	Classification	SVM,KNN,DT	★★★★	▲▲▲	■■❑	●●❍	[230]
	Reinforcement learning		ARAM-RL	★★★	▲▲▲△	■■■■❑	●●●❍	[231], [233], [234]
			Deep-RL	★★☆	▲▲▲▲	■■■■❑	●●●	[232]

Notes:
a) Deployability: ★ - poor, ★★☆ - moderate, ★★★★★ - excellent
b) Robustness: ▲ - poor, ▲▲△ - moderate, ▲▲▲▲▲ - excellent
c) Dataset limitations: ■ - little impact, ■■❑ - moderate impact, ■■■■■ - serious impact
d) Failure modes: ● - low sensitivity to model errors, ●●❍ - moderate sensitivity, ●●●●● - high sensitivity

rate (BER) below 1% even at a JSR of 60 dB. In addition, Yang et al. [239] utilized spatially distributed antennas on aircraft. One Earth-facing antenna captures pure interference signals, while a sky-facing antenna collects composite signals. Then, the CNN-based cancellation network reconstructs the navigation signal by canceling the received signals from these two antennas.

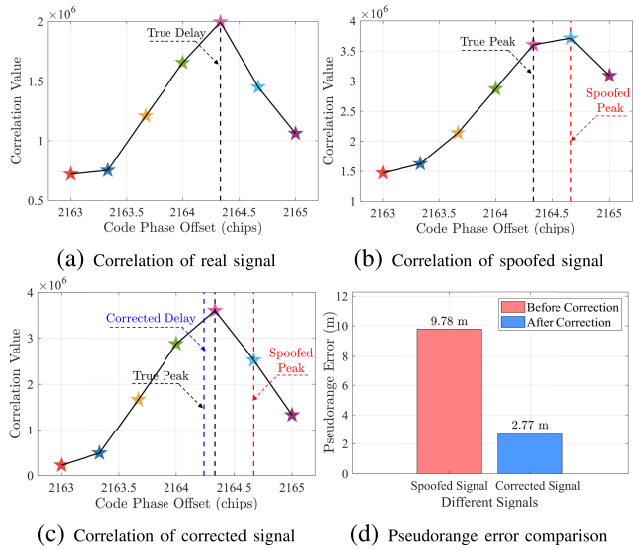
The indirect-prediction method is used to train networks to extract and isolate interference components from raw signals, although it typically requires prior knowledge of interference types. Xie et al. [215] developed an innovative LSTM-based array algorithm that uses the GNSS correlation integral gain as a loss function. By leveraging spatial correlation in array data to nonlinearly estimate aggregate interference, the method achieves simultaneous broadband suppression and a 24 dB improvement in the interference cancellation ratio (ICR). To address the challenges associated with separating mixed narrowband, linear sweep, and pulsed interference, Song et al. [240] proposed a time-frequency U-Net (TF-UNet) based on a CNN. The approach generates time-frequency spectra via high-resolution STFT and employs a U-Net architecture for precise interference feature segmentation. A signal fusion mechanism further enables effective interference suppression and GNSS signal reconstruction.

Signal separation and reconstruction can also be approached from a spatial perspective. Wentz et al. [241] proposed a classification-based transfer learning (CBTL) beamformer. A pretrained CNN is used for signal classification, and transfer learning is applied to optimize beamforming weights, enabling blind beamforming without prior knowledge of the array manifold. For a 4-element array, this method improves the output SINR by more than 8 dB. Uyen et al. [242] employed a CNN to directly estimate optimal beamforming weights from beam pattern images. The resulting patterns feature narrow main lobes and deep nulls, achieving an interference suppression ratio of -49.83 dB.

Furthermore, AI-based approaches support cognitive interference suppression frameworks that autonomously select antijamming strategies. Chen et al. [243] employed a pretrained GoogLeNet deep learning model to automatically select the optimal interference suppression method on the basis of time-frequency spectrum features. Compared with traditional methods, this approach improves suppression performance, with a CNR exceeding $38\ \mathrm{dB \cdot Hz}$, and demonstrates low sensitivity to interference parameters.

As shown in Table XIII, in terms of deployability, traditional supervised tools such as MLPs offer moderate performance because of their relatively simple architectures [214], whereas deep learning models exhibit lower deployability because of their high computational complexity and parameter counts. Thus, real-time implementation on resource-constrained platforms is challenging and often requires dedicated hardware acceleration [215]. With respect to robustness, DL techniques generally achieve good to high robustness. Models such as CNNs and LSTM networks excel at extracting complex features from jamming signals, enabling effective suppression across various interference types. However, DLs may display only moderate robustness in highly dynamic scenarios, as they are more sensitive to specific jamming patterns and parameter tuning [214], [215].

A major limitation of data-driven approaches is their strong dependence on data quality and scale, especially for deep learning models, the performance of which hinges on the availability of large, well-labeled training datasets [240]. Therefore, the performance of DLs significantly decreases when they encounter jamming patterns that are absent from the training data or under extreme signal-to-noise conditions [213]. In contrast, traditional supervised methods show moderately lower sensitivity; their failures are often more predictable and typically stem from inherent algorithmic limitations in modeling highly nonlinear interference dynamics [214].



(a) Correlation of real signal (b) Correlation of spoofed signal

(c) Correlation of corrected signal (d) Pseudorange error comparison

Fig. 10. Spoofing suppression using multicorrelator processing (code phase offset: 0.5 chips, JSR = 1.2 dB).

In summary, AI-based jamming mitigation via deep learning can be divided into two complementary paradigms defined based on their target objective and required prior knowledge. In the direct-prediction approach, the problem is treated as a regression or time series reconstruction task, where a neural network is trained to directly map interference-corrupted samples to the estimated clean GNSS signal. In contrast, in the indirect-prediction approach models are trained to explicitly estimate and then subtract the interference component from the composite signal. This method provides high interpretability and can leverage prior knowledge of interference types.

Both paradigms share a core trade-off; i.e., they deliver powerful, model-agnostic suppression capabilities and outperform many conventional model-based methods, but this comes at the cost of high computational demands for training and inference, a dependence on extensive and representative datasets, and difficulties in generalizing to interference types not adequately represented in the training data.

B. Spoofing Mitigation and Suppression

For spoofing suppression, the general approach involves separating the spoofing signals from the authentic signals or identifying the DOA of the spoofing transmitter and then using beamforming to attenuate signals arriving from that direction [244].

1) Signal Processing-Based Methods: In traditional signal processing, spoofing is suppressed by exploiting two properties: the creation of multiple correlation peaks and the introduction of consistent measurement errors. The uncorrelated characteristics between spoofing and authentic signals are also leveraged in this approach. We specifically discuss several methods as follows.

a) Multicorrelator processing: The use of multiple correlators to monitor correlation peaks allows for the detection and estimation of spoofing signal characteristics, reducing their impact on the phase estimation of authentic signals. The correlation values from each correlator can be used to reconstruct the peaks and gradually eliminate deceptive components, as illustrated in Fig. 10. Yang et al. [216] introduced the spoofing correlation peak cancellation (SCPC) method, which generates an inverse cancellation sequence to neutralize spoofing effects. When tested on the TEXBAT dataset, the SCPC corrects mixed signals, improves the CNR, and restores the correlation peak shape. Shang et al. [144] applied a robust extended Kalman filter to minimize the phase estimation errors of correlators, especially in dynamic environments. This approach reduced the position offset caused by spoofing from 600 m to approximately 20 m. Spoofing-induced correlation peaks can also be directly cancelled.

To tackle the detection difficulty cased by the similarity between repeater spoofing and multipath signals, Guo et al. [218] developed a multicorrelator tracking channel based on maximum likelihood estimation. After parameters such as the time delay and amplitude for each channel are estimated, a countersignal is added to recover the authentic signal. This method accurately estimates spoofing parameters with a delay of 0.6 chips and maintains positioning stability under both short-delay spoofing and long-delay spoofing. To achieve gradual spoofing suppression, Dabaghi et al. [217] integrated a multicorrelator structure with machine learning. An MLP network uses multicorrelator outputs to detect spoofing, while a Kalman filter estimates the DLL discriminator output, dynamically adjusting the code phase to suppress spoofing signals. In tests involving short-, medium-, and long-range bias scenarios, reliable positioning was achieved in 84.25%, 93.20%, and 97.24% of the cases after mitigation, respectively.

However, increasing the number of correlators not only improves detection and suppression performance but also increases system resource consumption and complexity [245]. Additionally, strong spoofing signals can suppress the correlation peaks of authentic signals, leading to erroneous estimation results.

b) Measurement correction: Spoofing signals received by adjacent receivers often originate from common interference sources, resulting in correlated measurement biases. Leveraging this inherent correlation, dual-frequency double-difference processing of pseudorange and carrier-phase measurements provides effective spoofing mitigation. By leveraging double-difference pseudorange and carrier-phase measurements from adjacent receivers, Stenberg et al. [219] detected spoofing signatures. This approach allows compromised measurements to be excluded from the positioning and timing solutions. Their results revealed that pseudorange double-differencing works for receivers spaced 20 m or more, whereas carrier-phase-based methods are suitable for shorter distances and require strict synchronization. When spoofing is detected, redundant GNSS measurements combined with Kalman filtering or nonlinear prediction models can be used to estimate and predict flight trajectories, ensuring that the results are spoofing-free [220].

To address the inability of traditional methods to correct signals during the initial deviation stage of synchronous spoofing, Fang et al. [223] exploited the oscillatory characteristics of the receiver's Doppler shift under spoofing and used nonlinear least-squares curve fitting to estimate authentic

signal parameters. This enabled spoofing mitigation before frequency lock through Doppler-smoothed pseudoranges and corrected code frequency. To improve estimation accuracy limited by correlator spacing, Jin et al. [222] first detected spoofing and performed a coarse estimation using a windowed sum of relative delays (WSRD) metric. An iterative strategy was then applied to refine the delay estimate beyond the correlator spacing limit. This approach was combined with an adaptive extended Kalman filter (AEKF) to handle abrupt changes in observation noise caused by spoofing. In contrast, Chen et al. [224] proposed a low-complexity method by leveraging the consistency between the code and carrier phases. They constructed a code-carrier difference (CCD) metric to estimate the pseudorange deviation directly, eliminating the need for multicorrelator parameter estimation. Their approach reduces the positioning error by up to 97.0% in the late-stage spoofing phase across various TEXBAT scenarios. Finally, to maintain measurement continuity after antispoofing, Sun et al. [221] implemented abnormal state prediction and feedback based on the vector tracking loop (VTL) through an extended Kalman filter (EKF), bridging signal interruptions through auxiliary channels and thereby preserving the continuity of PNT services.

In summary, the two primary signal processing-based spoofing mitigation methods operate at fundamentally different layers of the receiver chain, each with distinct trade-offs among performance, complexity, and hardware dependence. Multicorrelator processing functions at the correlation level within a single receiver. While more correlators increase suppression performance, they also linearly increase computational and resource costs. Furthermore, efficacy can decrease when spoofing signals are strong enough to dominate or suppress the authentic correlation peak. In contrast, measurement correction is implemented at the positioning solution level, requiring data from multiple spatially separated receivers or antennas. The effectiveness and applicability of this method are directly governed by the antenna spacing and synchronization quality.

Therefore, the choice hinges on the operational constraint; i.e., multicorrelator processing offers a self-contained, receiver-integrated solution at the cost of internal computational resource and robustness against very strong spoofers, whereas measurement correction provides a robust and geometry-based exclusion method at the expense of external hardware configuration.

2) Array Antennas-Based Methods: Unlike jamming, spoofing is mostly addressed through spatial filtering rather than time- and frequency-domain filtering [225]. By leveraging the characteristic that spoofing signals are typically emitted from a single direction, multiantenna systems can detect spoofing through DOA correlations. Once the angle of arrival differs between authentic and spoofing signals, multiple antennas can form adaptive beams to nullify spoofing from common directions while preserving the GNSS signals [226]. Arribas et al. [228] proposed an intelligent antenna architecture based on antenna arrays. It estimates the DOA to identify spoofing signals and adaptively nulls interference in the corresponding direction.

Noh et al. [227] evaluated arrays with varying numbers of antenna elements for spoofing mitigation. They reported that increasing the number of elements enhances suppression, but performance gains diminish as the spoofing-to-authentic signal power ratio narrows. With respect to repeater spoofing, which is correlated with authentic signals, Ren et al. [246] analyzed the performance of multibeam antijamming receivers. Their results showed that the MVDR algorithm consistently suppresses spoofing below the authentic signal power level, with higher spoofing power yielding better suppression.

When the spoofing signal power is close to that of an authentic signal, distinguishing spoofing from multipath effects is challenging. Zhao et al. [247] employed an improved feature space spectrum method with signal preprocessing, such as self-coherence denoising and forward-backward spatial smoothing, to estimate the DOA of all incident signals. They combined power estimation and cross-correlation peak monitoring to detect spoofing and used subspace projection and beamforming for interference suppression. For multidirection collaborative spoofing attacks, Venturino et al. [229] utilized phase difference measurements from antenna arrays integrated with navigation filter state estimation. They design a generalized likelihood ratio test to detect spoofing signals. An adaptive resilience navigation filter (ARNF) was proposed to dynamically estimate the bias introduced by spoofing and adjust the measurement model for suppression. The ARNF accurately detects multiple spoofing attacks (e.g., four signals) and estimates biases to improve positioning accuracy.

In summary, array-based spoofing mitigation primarily involves spatial filtering, but diverging strategies regarding hardware reliance and algorithmic sophistication are used. Increasing the number of antenna elements enhances suppression but at the cost of greater hardware complexity, size, and power consumption, which is a critical constraint for UAVs. Moreover, performance gains diminish as the spoofing-to-authentic signal power ratio decreases, revealing a fundamental sensitivity limit. This reflects an overarching trade-off between achieving better performance through increased hardware resources and developing more intelligent, adaptive algorithms to maximize capability within strict SWaP limits.

3) Artificial Intelligence-Based Methods: For spoofing mitigation, AI methods primarily exploit the correlations between signals and measurement outputs to mitigate the impact of spoofing signals on true measurements.

a) Machine learning: In scenarios with limited dynamics, this approach is similar to spoofing detection; i.e., after identifying malicious measurements, anomalous values re systematically discarded. Pardhasaradhi et al. [230] distinguished authentic and spoofing signals by analyzing received signal power and correlation peak changes. They leveraged machine learning algorithms such as an SVM and a KNN to screen out spoofing-affected measurements and select the best ones for position estimation on the basis of the relationship between measurements and features.

b) Reinforcement Learning (RL): For dynamic spoofing scenarios, RL can compensate for trajectory deviations caused by spoofing-induced position and attitude changes during UAV flights [231]. Eldosouky et al. [234] proposed an active defense

framework based on cooperative localization to counter stealth spoofing attacks, with the attacker-defender interaction modeled as a dynamic Stackelberg game. Their approach can protect all drones in a swarm when the spoofing signal induces a positional deviation of up to 60 meters by employing a Stackelberg equilibrium strategy. Tang et al. [232] introduced a deep RL-based positioning correction algorithm featuring adaptive reward augmentation (ARAM) to improve GNSS accuracy. By learning the nonlinear mapping between measurements and positioning outputs, ARAM effectively mitigates spoofing-induced biases and enables real-time trajectory correction.

To reduce the resource consumption of RL models, Hu et al. [233] proposed a lightweight and integrated RL framework. It dynamically selects between GPS-based and vision-based navigation strategies and incorporates an improved prioritized experience replay mechanism based on past incorrect decisions. For three types of spoofing attacks (random, replay, and covert), the system achieves an average detection accuracy exceeding 96% and a task completion rate over 91%, with an average real-time decision latency below 23 ms.

Moreover, the learning abilities of artificial intelligence methods can be integrated with signal reconstruction techniques from compressive sensing (CS). Wang et al. [248] combined a spiking neural network (SNN) with compressive sensing. The SNN learns the characteristics of spoofing-free cross-ambiguity functions (CAFs) to detect spoofing. Subsequently, an improved sparse Bayesian learning (ISBL) algorithm performs sparse reconstruction of the time-domain autocorrelation function (TACF). By constructing an over-complete dictionary, the received signal is decomposed into parameterized combinations of authentic and spoofing components. The reconstructed spoofing component is then subtracted to recover the authentic signal.

As shown in Table XIII, traditional supervised learning classifiers demonstrate advantages for integration into real-time, resource-constrained systems such as UAVs with minimal hardware overhead because of their relatively simple architecture and low computational demands [230]. In contrast, RL and Deep-RL methods with more complex network structures often require specialized hardware acceleration in practical implementations, posing significant challenges to edge deployment [233]. With respect to robustness, Deep-RL methods achieve superior performance by learning adaptive policies that can effectively counter dynamic and evolving spoofing tactics through continuous environmental interaction [232]. However, the robustness of supervised classifiers is moderate, as they may struggle to generalize to novel and sophisticated spoofing strategies not represented in their training data [230].

As mentioned, the severe limitations of datasets profoundly impact most data-driven approaches, particularly deep learning and reinforcement learning (RL) models. These models heavily rely on large-scale, high-quality, and representative training data to comprehensively cover potential spoofing scenarios and signal conditions [232]. Their performance can significantly decrease, such as unexpected erroneous feedback and judgments, when the training data lack diversity or fail to encompass real-world operational variations. In contrast, the failures of supervised models in such cases are often relatively predictable, as they primarily stem from the inherent limitations of the algorithms [230].

In summary, AI-based spoofing mitigation methods employ a versatile, data-driven paradigm that operates across the measurement and positioning layers, and the nonlinear mapping relations between corrupted inputs and corrected navigation states are learned. In low-dynamic scenarios, methods based on features such as signal power and correlation peak distortion, such as using an SVM or a KNN, provide a selective filtering approach to identify and discard spoofed measurements. For high-dynamic scenarios involving UAVs, RL and Deep-RL frameworks (e.g., with adaptive reward augmentation) support active trajectory correction by learning to compensate for spoofing-induced deviations in real time. This reflects a key contrast: static or low-dynamic methods focus on measurement classification and exclusion, whereas dynamic methods shift toward continuous control and state recovery.

In addition, AI methods for spoofing mitigation inherit the common AI trade-offs of computational cost, dependence on extensive and representative training data, and potential challenges in real-time deployment on resource-constrained platforms. Thus, AI-based mitigation is most advantageous in scenarios where spoofing patterns are sophisticated, variable, or poorly characterized by traditional models, provided that sufficient onboard processing and learning data are available.

4) System Integration-Based Methods: As a system of independent sensors, the INS can provide high-precision state information in the short term and is immune to spoofing. Beyond spoofing detection, integrated GNSS/INS navigation systems can also utilize information updates to achieve spoofing mitigation. Huang [235] proposed an INS-aided tracking (INSAT) framework based on robust Kalman filtering for spoofing suppression. This framework uses INS-derived short-term precise states to support and adaptively adjust the GNSS receiver's tracking loops, thereby maintaining lock on the authentic signal. Evaluated on the TEXBAT dataset, INSAT reduced the maximum positioning error under spoofing from 600 m to within 12 m, achieving a 98% error reduction. In slow spoofing scenarios with an average speed of $0.5\ \mathrm{m/s}$, its the maximum error is only 20.3% of that of a multicorrelator mitigation algorithm. The framework also sustains authentic-signal tracking during spoofing pulls and supports subsequent INS error correction, preventing divergence under prolonged attacks.

Spoofing can also disrupt the high-precision positioning of RTK/INS tightly coupled systems, where traditional EKF suffer from noise-statistics mismatch and frequent AR failures, leading to state estimation divergence. To address this, Hao [236] proposed a joint strategy combining an adaptive robust Kalman filter (ARKF) with partial ambiguity resolution (PAR). The ARKF performs float estimation, the PAR achieves a fixed solution, and INS errors are used for dynamic compensation. The ARKF+PAR method reduces the 3D position error (RMS) from 23.60 m to 1.03 m, significantly enhancing system reliability.

Against advanced spoofing strategies, such as targeted spoofing and jamming-spoofing hybrid attacks, traditional GNSS/INS methods suffer from low detection probability

and ineffective mitigation. Shang et al. [237] integrated the multipath estimation delay lock loop (MEDLL) approach with the INS. Their approach uses multiple correlators to estimate signal parameters (delay, amplitude, phase) and separates spoofing from authentic components via maximum likelihood estimation. Moreover, the INS is used to predict pseudorange errors and cancel the spoofing-induced component.

To counter spoofing attacks that exploit system vulnerabilities, such as periods of low LiDAR reliability for covert vehicle deviation, Chang [238] proposed an improved Kalman filter model that uses measurement variance monitoring (MVM) to monitor innovation changes. When spoofing causes innovation anomalies, the MVM constrains the impact of GNSS outliers on the fusion filter. The proposed minimum covariance constraint method (MCCM) imposes a lower bound on the position-related covariance matrix, enhancing the corrective capability of the LiDAR between GNSS signals to improve robustness. When evaluated using the KAIST real-world dataset in both open-sky and urban canyon scenarios, this model reduces the maximum lateral deviation from 11.34 m (using a traditional loosely coupled method) to 1.79 m.

In summary, in system-integrated spoofing mitigation, primarily through GNSS/INS coupling, the INS's spoofing-immune, short-term high-fidelity motion estimates are used to correct the GNSS solution, fundamentally altering the mitigation paradigm from signal-domain excision to state-domain robustness. This approach can be applied at the tracking loop level, as in the INSAT framework, which uses INS data to adaptively adjust receiver tracking parameters and assist in locking onto the authentic signal. Alternatively, integration occurs at the fusion filter level, e.g., MEDLL with the INS. Collectively, these tightly coupled methods demonstrate that leveraging the complementary strengths of the INS and GNSS provides a powerful, system-level defense that is highly effective against both simplistic and sophisticated spoofing attacks.

C. Performance Evaluation and Selection Guidelines

To compare the specific differences among various techniques, methods are evaluated using a unified framework based on four key metrics in this section: suppression capability, position recovery capability, computational load, and deployment readiness. A consolidated assessment is presented in Table XII. The following analysis synthesizes the performance trade-offs for jamming and spoofing mitigation, culminating in practical selection guidelines for UAV platforms.

1) Techniques for Jamming:

a) Cross-method comparative analysis: The evaluation reveals clear trade-offs among performance, resource cost, and application scope. Notch filters and TF transforms excel against narrowband jamming based on interference sparsity. However, their efficacy diminishes in cases with broadband jamming, and their position recovery is moderate, as signal distortion can introduce biases. Although the TF transform yields better jamming suppression performance than notch filters, it is more complex than basic notch filters are. Array signal processing achieves the highest suppression capability for both narrowband and broadband jamming and offers excellent signal preservation but at the cost of a high computational load and the requirement of multiple antennas. Deep learning methods yield strong, generalized suppression but currently lag in position recovery, as signal reconstruction remains a challenge. Their most significant drawback is the very high computational load, although deployment can range from single-antenna systems to multiantenna systems.

b) Selection advice for UAV platforms: Medium-size UAVs with high payloads and power capacities can support the most effective solutions. Array signal processing is the optimal choice for robust, high-performance suppression in contested environments, justifying its hardware and computational cost. DL-based methods present powerful, adaptive alternatives, especially against unknown or complex jamming, provided that sufficient onboard processing is available for model inference.

However, for small UAVs under strict SWaP constraints, efficiency is paramount. Notch filters are the default, low-complexity solution for narrowband jamming. For more complex or mixed threats, TF transforms offer a balanced increase in capability with a manageable increase in computational load. DL is generally infeasible unless highly optimized, lightweight models are deployed.

2) Techniques for Spoofing:

a) Cross-Method comparative analysis: Spoofing mitigation methods exhibit a wide range of hardware dependencies and operational principles. Multicorrelator processing provides good suppression and recovery but imposes a high computational load and requires specialized receiver hardware. Measurement correction directly enables high-integrity positioning by excluding faulty measurements but supports limited suppression. Array signal processing again offers a strong spatial filtering solution but depends on multiantenna hardware. AI methods clearly improve performance. Supervised learning methods display good performance with moderate cost, whereas deep learning achieves the highest scores at the cost of the highest computational demand. The integrated systems approach offers the highest theoretical suppression capability and robust position recovery, but it requires additional sensors, making it a resource-intensive, system-level solution.

b) Selection advice for UAV platforms: For medium UAVs, these platforms can leverage high-performance, multisensor solutions. Array signal processing is highly effective if hardware resources permit. Besides, DL-based mitigation represents the state-of-the-art approach for countering sophisticated spoofing strategies. Meanwhile, system integration provides the ultimate robustness for critical missions, assuming that the platform can be equipped with additional sensors and corresponding data processing. Alternatively, a hybrid approach, such as using measurement correction with a multiantenna setup, provides robust, geometry-based integrity.

For small UAVs, practicality and ease of integration are key considerations. Supervised learning provides an excellent balance of good performance, low computational cost, and minimal hardware needs. But multicorrelator techniques are less ideal because of specialized receiver hardware requirements. In cases where real-time performance is not highly

TABLE XIV
METRICS OF INTERFERENCE MITIGATION AND SUPPRESSION

Types	Specific Tech-niques	Suppression capability	Positiong recovery capability	Computa-tional load	Deploy-ment readiness
Jamming	Notch filter	NB:★★★☆ BB:★★	NB:▲▲▲△ BB:▲▲	■■	A
	TF Transform	NB:★★★★ BB:★★★☆	NB:▲▲▲△ BB:▲▲△	■■❑	A
	Array signal processing	NB/BB: ★★★★★	NB/BB: ▲▲▲△	■■■	B
	Deep learning	NB/BB: ★★★★☆	NB/BB: ▲▲▲	■■■■■	A/B
Spoofing	Multi-correlators	★★★☆	▲▲▲△	■■■■	C
	Measurement correction	★★☆	▲▲▲	■■■■	A/B/C
	Array signal processing	★★★☆	▲▲▲△	■■■❑	B
	Supervised learning	★★★★	▲▲▲▲	■■■	A
	Reinforcement learning	★★★★☆	▲▲▲▲△	■■■■■	A/B
	GNSS/INS	★★★★★	▲▲▲△	■■■	C/D

Notes:
a) Suppression capability: ★ - low, ★★☆ - moderate, ★★★★★ - high
b) Location recovery capability: ▲ - low, ▲▲△ - moderate, ▲▲▲▲ ▲ - high
c) Computational load: ■ - low, ■■❑ - moderate, ■■■■■ - high
d) Deployment readiness: A - Single antenna, B - multi antennas, C - special receivers, D - other sensors
e) NB: narrowband jamming BB: broadband jamming

needed, the measurement correction method can also be adopted. The low-cost GNSS/INS solution may be constrained by device performance, resulting in certain limitations in terms of interference suppression and positioning recovery capabilities.

In summary, the optimal mitigation strategy is dictated by a core trade-off: high-performance methods (e.g., array processing and DL methods) demand significant hardware and computational resources, whereas more resource-efficient methods (e.g., notch filters and ML methods) involve concessions in suppression breadth or recovery fidelity. For jamming, the choice is driven primarily by the jammer's spectral characteristics and platform resources. For spoofing, the choice further depends on the available sensor configuration (e.g., number of antennas or receivers) and the required level of solution integrity. There is no universal best method; the selection must align the technique's inherent strengths and costs with the UAV's operational constraints and mission threat profile.

VI. CURRENT CHALLENGES RELATED TO SATNAV ANTI-INTERFERENCE

As mentioned in Sections IV and V, a comprehensive technology system has been established for addressing jamming and spoofing, spanning from interference detection and identification to mitigation and suppression. Table XV presents a comparative analysis of current navigation interference countermeasures for UAVs, summarizing and evaluating the characteristics, performance and feasibility of each category.

Traditional signal-processing methods operate at the signal level with low hardware demands and moderate computational cost, but offer limited robustness against unknown or dynamic interference. Array antenna-based approaches leverage spatial filtering, providing enhanced performance at the expense of higher hardware complexity (e.g., multiple antennas and RF channels) and substantial computational load for real-time covariance estimation. Similarly, AI-based methods incur high computational costs during training and inference and exhibit strong dependence on representative training data. However, once deployed, AI models can capture subtle signal characteristics for superior performance while only occupying storage memory. Consequently, for resource-constrained consumer UAVs, lightweight signal processing remains practical for basic detection and evasion. In contrast, industrial-grade platforms with greater payload and computing resources can integrate small antenna arrays and AI models to handle complex interference in tactical scenarios.

Although these methods exhibit distinct advantages and have been partially deployed in practice, significant challenges persist in achieving robust interference detection and mitigation for UAV operations, particularly in increasingly complex and noncooperative interference environments. The primary implementation challenges of the existing navigation countermeasures for UAV deployment are summarized as follows.

A. Technical Bottlenecks Under Onboard Resource Constraints

The primary challenge in achieving robust UAV navigation interference resistance is related to onboard resource constraints (e.g., payload, computing resources, and power output) [249]. These constraints hinder the implementation of existing interference countermeasures because of their hardware and algorithmic complexity.

As shown in Table XV, although array antennas demonstrate effectiveness in interference detection and mitigation, they impose significant computational loads and require specific antenna hardware configurations. However, the limited payload of UAVs prevents them from carrying arrays with multiple elements. This constraint limits the signal gain and directivity of antennas, degrading the actual performance of array-based methods [250].

Advanced methods such as signal separation and the reconstruction of AI-based methods require substantial amounts of computing and storage resources, as indicated in Table IX and Table XII. This creates a significant implementation bottleneck for resource-constrained UAV platforms [251]. Furthermore, battery capacity and low power output restrict the use of interference suppression devices. Therefore, the high hardware and software demands of existing interference countermeasures are often incompatible with the resource-constrained reality of UAVs, hindering the improvement of their navigation and antijamming capabilities.

TABLE XV
ANALYSIS OF PERFORMANCE AND FEASIBILITY FOR INTERFERENCE COUNTERMEASURES

Methods	Interference types	Overall efficacy	Computational load	Hardware requirements	Robustness against evolving threats	SWaP	Theoretical feasibility	Actual feasibility
Signal processing	Jamming	★★★☆	★★	★★	★★	S: ●● W: ●● P: ●●	■■■❑	■■■
	Spoofing	▲▲	▲▲△	▲▲	▲△		◆◆◆◇	◆◆◆
Array antennas	Jamming	★★★★☆	★★★☆	★★★★	★★★★	S: ●●● W: ●●● P: ●●○	■■■■	■■■❑
	Spoofing	★★★☆	★★★☆	★★★★	★★★		◆◆◆	◆◆◇
Artificial intelligence	Jamming	★★★★	★★★★☆	★★★	★★★☆	S: ●●○ W: ●○ P: ●●●○	■■■❑	■❑
	Spoofing	★★★★☆	★★★☆	★★★	★★★★		◆◆◆◆	◆◆◆◇

Notes:
Evaluation metrics for jamming: ★ - low ★★☆ - medium, ★★★★★ - high
S: Size W: Weight P: Power
Feasibility to jamming: ■ - low, ■■❑ - medium, ■■■■■ - high
SWaP cost: ● - low, ●●○ - medium, ●●●●● - high
Feasibility to spoofing: ◆ - low, ◆◆◇-medium, ◆◆◆◆◆ - high

B. Insufficient Flexibility of Existing Countermeasures

A robust anti-interference system requires considerable flexibility, such as the ability to dynamically adapt its countermeasures in real time when encountering unknown interference. However, the emergence of dynamic and covert interference poses significant challenges to conventional approaches, which often fail to meet the real-time and adaptive response requirements of navigation.

Conventional countermeasures were typically based on a cascaded "detect-then-suppress" processing chain. This structure introduces inherent latency, limiting the real-time response under dynamic interference conditions [20]. In addition, as discussed in Sections IV and V, existing techniques often exhibit applicability to specific types. For example, time-frequency filtering with a single antenna effectively suppresses narrowband jamming but performs poorly against broadband jamming.

Data-driven artificial intelligence methods demonstrate strong performance in complex interference environments. Nevertheless, their effectiveness highly relies on training data quality and coverage [183]. The absence of comprehensive datasets encompassing jamming, spoofing, and emerging threats specific to UAV navigation restricts model generalizability. Thus, performance degrades significantly when real-world interference falls outside the training data distribution.

Moreover, compared with traditional signal processing or array antenna techniques, AI-based methods generally require more computational and memory resources. However, the limited processing capabilities and memory of UAVs render the real-time execution of complex AI algorithms infeasible [252]. Furthermore, the prevalent offline training paradigm restricts the model's ability to adapt to dynamic interference in real time. Additionally, current AI approaches typically leverage features from either the signal layer or the vehicle behavior layer independently. The lack of deep fusion across these layers hinders further advancements in AI-driven interference mitigation.

C. Deficient UAV-Specific Strategies for GNSS Anti-Interference

The current methods of enhancing UAV navigation in interference-prone environments fall into two main categories. The first is onboard integrated navigation, which combines multisource systems such as the GNSS, IMU, and vision. This strategy uses systems immune to electromagnetic interference to maintain continuous navigation when the GNSS signal is denied [253]. However, this approach is limited by the inherent drawbacks of alternative systems, such as error accumulation in inertial navigation and visibility dependence in visual navigation.

Methods in the second category employ conventional detection and suppression at the signal-processing level. As shown in Table XV, the performance of these methods is constrained by the specific characteristics of the UAV platform. In addition, most current approaches focus specifically on suppressing either jamming or spoofing attacks and lack comprehensive coverage to handle varied interference scenarios effectively.

Both aforementioned strategies address interference at the signal or information level but do not incorporate the unique flight maneuvering characteristics of UAVs. As a result, a dedicated and comprehensive interference-handling solution for UAV satellite navigation systems is currently lacking.

Additionally, as UAVs now face increasingly complex and adaptive interference patterns that evolve dynamically during interference-countermeasure engagements, the malignant effects caused by the inadequate design become more severe. In contested environments such as military operations, UAVs often encounter hybrid attacks combining jamming and spoofing. Existing strategies often fail to ensure mission completion under such conditions. Therefore, dedicated interference-handling solutions for UAV satellite navigation systems are needed to ensure resilient response capabilities.

D. Emerging Challenges in UAV Swarm-Based Anti-Interference

While the limitations of countermeasures at the individual UAV platform level were analyzed in previous subsections, in this subsection, focus is shifted to the UAV swarm level. In several studies, anti-interference research has been conducted based on UAV swarms.

For instance, Michieletto et al. [101] analyzed received signal strength (RSS) measurements among UAVs to achieve reliable UAV self-positioning. Zhou et al. [254] proposed

a cooperative beamforming technique in which interference signals received by collaborative UAVs are aggregated and suppressed at a reference node through frequency-domain power inversion. Moreover, this approach is complemented by a least-squares-based collaborative positioning algorithm, fully exploiting the multinode characteristics of the swarm to enhance overall localization accuracy and resilience [255].

However, the dynamic and large-scale nature of UAV swarms introduces complexity in real-time information fusion and distributed decision-making, often leading to latency in the interference response. Additionally, maintaining secure and reliable interdrone communication under sophisticated interference remains problematic, as adversarial attacks may exploit vulnerabilities in cooperative perception or data-sharing mechanisms.

When critical nodes are compromised, insufficient system redundancy reduces resilience. Moreover, adaptive hybrid interference overwhelms current static mitigation frameworks, requiring intelligent and self-organizing solutions. Thus, future efforts must be made to address these issues through lightweight distributed learning, resilient communication protocols, and hierarchical swarm control architectures.

These four challenges form an interdependent hierarchy. Fundamental onboard resource constraints directly limit the flexibility and real-time performance of countermeasures. This scarcity further contributes to the lack of UAV-specific strategies, as most solutions are generic adaptations rather than codes designed for the unique dynamics and SWaP limits of different platforms. When scaling to the swarm level, these individual platform limitations are compounded, introducing new complexities in terms of coordination latency, communication security, and system resilience. These complexities thereby require more sophisticated but still resource-aware solutions.

VII. Future Directions in UAV GNSS Anti-Interference

Given the current countermeasure limitations, future research can be conducted at the signal, algorithm, and system levels to provide systematic protection for safe and reliable UAV navigation in interference-prone environments, as illustrated in Fig. 11.

A. Robustness Enhancement for Signal Reception

The main goal is to increase the signal power and redundancy at the RF front end of the receiver, thereby increasing the reception robustness by reducing the impact of interference at the signal level.

1) Cost-Effective Compact Array Robust Reception: Although conventional array processing is effective, it is difficult to implement under payload limitations. Optimizing the array antenna design can help promote good performance in cases with small arrays or tight spacing. This requires antenna coupling and achieving a balance between computational complexity and anti-jamming effectiveness [250]. Reducing the number of elements while maintaining anti-jamming performance remains a key challenge. A promising

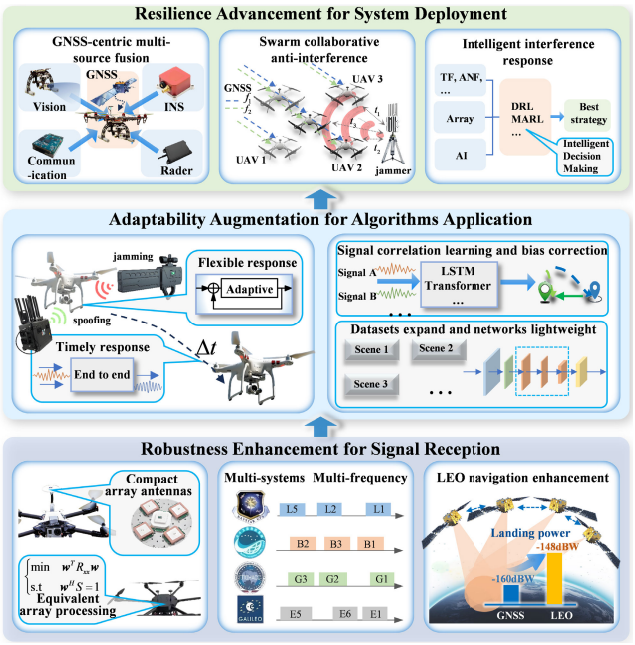


Fig. 11. Technological roadmap for future GNSS interference countermeasures in UAV navigation systems.

and cost-effective pathway is to leverage the RTK dual-antenna systems commonly equipped on UAVs to enhance anti-interference performance. The key to realizing this potential lies in addressing the issue of signal phase distortion during this process.

2) Multifrequency and Multisystem Signal Redundancy: The high integration of current processing chips enables the simultaneous reception of signals from multiple satellite systems and across multiple frequency bands [256]. When interference affects a specific frequency band, navigation can continue using signals from other bands. Furthermore, interference characteristics can be identified via joint analysis of multisystem signal measurements [257]. Multiconstellation positioning also increases signal availability in complex electromagnetic environments, ensuring a sufficient number of satellite signals for positioning during band-specific interference.

3) Low-Earth-Orbit Satellite Signal Navigation Enhancement: Compared with traditional MEO signals, current low-Earth-orbit (LEO) satellites, with their navigation-enhancement services, can significantly increase the received power [258]. Their close-proximity orbits and large-scale constellation coverage can accelerate the convergence of precise point positioning (PPP), enabling rapid and accurate positioning that meets the real-time response needs of UAVs [259]. This allows user terminals, especially UAV swarms, to access numerous satellites simultaneously.

B. Adaptability Augmentation for Algorithm Application

The current interference-resistance algorithms could be improved from two aspects: *i)* enhancing the adaptability of traditional methods and *ii)* expanding and refining deep-learning algorithms for better interference-countering performance.

1) Counteracting Complex Interference With Adaptive Anti-Interference: To address the complex interference challenges associated with UAVs, flexible countermeasures are essential to handle adaptive or covert interference. By leveraging cognitive intelligent decision-making based on interference perception, appropriate suppression methods can be selected. The development of unified approaches and end-to-end detection-mitigation systems can meet the real-time response needs of UAVs.

2) Improvement in the Application of AI Methods: AI-based methods can be further applied to learn signal correlations and correct measurement biases caused by signal distortion from interference. Existing datasets need to be expanded to include more interference types to improve model adaptability and generalizability. With respect to network design, lightweight networks such as attention-enhanced or parameter-pruned transformers can be used for efficient feature extraction [260]. Modular hybrid network architectures with partially iteratively trained layers can improve model adaptability to emerging interference [261]. Finally, knowledge distillation can be used to compress pretrained models for UAV deployment, reducing complexity while retaining performance [262].

C. Advances in Resilience for System Deployment

Leveraging multisensor fusion, swarm collaboration, and intelligent countermeasures provides a viable path for significantly enhancing navigation resilience at the system level.

1) GNSS-Centric Multisource Deep Fusion: Current multisensor fusion-based UAV navigation technologies are limited by the shortcomings of individual systems, leading to performance degradation. To enhance navigation reliability, GNSS-centered data fusion methods, including model-based approaches such as Kalman filters and factor graphs, as well as learning-based approaches, could be adopted [263]. With the GNSS providing absolute positioning capability and other systems offering redundant information, this fusion approach ensures a correct position reference to enhance overall anti-interference capabilities.

2) Swarm-Based Collaborative Interference Countermeasures: The collaboration of UAVs in a swarm involves integration of the time, frequency, and power domains to enable multidimensional countermeasures to be implemented. However, the selection of information transmission and fusion strategies, as well as effective methods to enhance system redundancy, still requires in-depth research [264]. Future swarm anti-interference systems may integrate distributed learning to reduce the computational loads of UAVs [265]. Federated learning can also be deployed to enhance interdrone data transmission security [174].

3) Intelligent Response Strategies to Interference: Machine learning has been widely used in GNSS applications (e.g., signal acquisition and integrated navigation) [266]. For UAV adversarial decision-making, a perception-decision closed-loop architecture can be constructed with machine learning techniques [267]. The perception module identifies interference patterns in real time through a time-frequency analysis network, and the decision-making module uses deep reinforcement learning to generate optimal countermeasures. By combining deep reinforcement learning and transfer learning, UAVs can make timely, targeted decisions during dynamic flight maneuvers [268]. As a result, UAV computing resources can be optimized, and trajectory prediction can be further improved, collectively enhancing the system's resilience to interference attacks.

VIII. Conclusion

This survey comprehensively reviews interference threats to UAV satellite navigation systems and their corresponding countermeasures. By analyzing system vulnerabilities and summarizing the practical lessons learned, it highlights the critical need to enhance navigation availability in contested environments. Beyond characterizing conventional jamming and spoofing, Section III introduces emerging interference paradigms. It also summarizes distinct threats and existing countermeasures across different UAV operational scenarios.

The current approaches used to address GNSS interference primarily revolve around detection and mitigation. Jamming is typically detected via anomalies in signal distribution and suppressed using spatial or temporal filtering. Spoofing is identified through measurement inconsistencies and mitigated by signal validation or measurement correction. The established methods include traditional signal processing, array antenna, and artificial intelligence techniques. Following a detailed review and comparison in Sections IV and V, the characteristics and performance metrics of these methods are systematically summarized, providing guidance for selecting suitable technologies in various UAV scenarios.

Our research indicates that the existing signal processing and array antenna methods have matured into established frameworks for interference detection and suppression. While AI methods often outperform traditional approaches in detection and identification due to their superior feature extraction capabilities, their application in interference mitigation remains in an exploratory and developmental stage. We conducted a targeted comparative analysis of AI methods, emphasizing robustness and practical deployability. Furthermore, on the basis of the comparative analysis of existing technologies, Section VI presents a comprehensive examination of challenges spanning from different levels in UAVs.

To address the current UAV navigation challenges in interference-prone environments, we propose a hierarchical enhancement framework that integrates signal, algorithm, and system layers. The signal layer combines multifrequency, multisystem reception with LEO augmentation, and compact antenna array processing to enhance redundancy and cost-effectiveness. At the algorithm layer, dynamic anti-interference strategies integrate advanced architectures such as Transformer models for end-to-end interference suppression. System-level optimization establishes a GNSS-centered multisource fusion architecture that exploits swarm intelligence and adaptive decision-making to enable collaborative countermeasures under resource constraints. This multilayered approach ensures comprehensive interference resistance, fulfilling the safety requirements for UAV navigation in complex electromagnetic environments.

REFERENCES

[1] Y. Tamanna. (May 2024). *Drone Report 2024*. [Online]. Available: https://www.startus-insights.com/innovators-guide/drone-report/

[2] N. Elmeseiry, N. Alshaer, and T. Ismail, "A detailed survey and future directions of unmanned aerial vehicles (UAVs) with potential applications," *Aerospace*, vol. 8, no. 12, p. 363, Nov. 2021.

[3] *Civilian Drone Market Report: Trends, Forecast and Competitive Analysis to 2030*. Accessed: Oct. 23, 2025. [Online]. Available: https://www.giiresearch.com/report/luci1418473-civilian-drone-market-report-trends-forecast.html

[4] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, "Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends," *Intell. Service Robot.*, vol. 16, no. 1, pp. 109–137, Mar. 2023.

[5] K. Al-Dosari, Z. Hunaiti, and W. Balachandran, "Systematic review on civilian drones in safety and security applications," *Drones*, vol. 7, no. 3, p. 210, Mar. 2023.

[6] M. Miriam. (May 2024). *The Rise of Tiny FPV Drones in Warfare: How They're Used*. [Online]. Available: https://dronelife.com/2024/05/31/the-rise-of-tiny-fpv-drones-in-warfare-how-theyre-used/

[7] P. Cao et al., "Computational intelligence algorithms for UAV swarm networking and collaboration: A comprehensive survey and future directions," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 4, pp. 2684–2728, 4th Quart., 2024.

[8] G. W. Hein, "Status, perspectives and trends of satellite navigation," *Satell. Navigat.*, vol. 1, no. 1, p. 22, Dec. 2020.

[9] S. Czyża, K. Szuniewicz, K. Kowalczyk, A. Dumalski, M. Ogrodniczak, and Ł. Zieleniewicz, "Assessment of accuracy in unmanned aerial vehicle (UAV) pose estimation with the REAL-time kinematic (RTK) method on the example of DJI matrice 300 RTK," *Sensors*, vol. 23, no. 4, p. 2092, Feb. 2023.

[10] F. Nex et al., "UAV in the advent of the twenties: Where we stand and what is next," *ISPRS J. Photogramm. Remote Sens.*, vol. 184, pp. 215–242, Feb. 2022.

[11] M. Felux, P. Fol, B. Figuet, M. Waltert, and X. Olive, "Impacts of global navigation satellite system jamming on aviation," *NAVIGATION, J. Inst. Navigat.*, vol. 71, no. 3, 2024, Art. no. navi.657.

[12] E. Ghizzo, E.-M. Djelloul, J. Lesouple, C. Milner, and C. Macabiau, "Assessing jamming and spoofing impacts on GNSS receivers: Automatic gain control (AGC)," *Signal Process.*, vol. 228, Mar. 2025, Art. no. 109762.

[13] R. Sabatini, T. Moore, and S. Ramasamy, "Global navigation satellite systems performance analysis and augmentation strategies in aviation," *Prog. Aerosp. Sci.*, vol. 95, pp. 45–98, Nov. 2017.

[14] Z. Wang, R. Liu, Q. Liu, L. Han, and J. S. Thompson, "Feasibility study of UAV-assisted anti-jamming positioning," *IEEE Trans. Veh. Technol.*, vol. 70, no. 8, pp. 7718–7733, Aug. 2021.

[15] A. Ranganathan, A. Belfki, and P. Closas. (May 2024). *Breaking the Formation: The Impact of GNSS Spoofing on UAV Swarms*. [Online]. Available: https://insidegnss.com/breaking-the-formation-the-impact-of-gnss-spoofing-on-uav-swarms/

[16] A. Novák, K. Kováčiková, B. Kandera, and A. N. Sedláčková, "Global navigation satellite systems signal vulnerabilities in unmanned aerial vehicle operations: Impact of affordable software-defined radio," *Drones*, vol. 8, no. 3, p. 109, Mar. 2024.

[17] S. Madry, "National and international governmental policy issues PNT frequencies, overlap, and spectrum issues: International PNT issues," in *Global Navigation Satellite Systems and Their Applications*. Cham, Switzerland: Springer, 2024, pp. 95–107.

[18] (Jun. 2024). *Easy Access Rules for Unmanned Aircraft Systems (Regulations (EU) 2019/947 and 2019/945)—Revision From July 2024—Available in Pdf, Xml, and Online Format — EASA*. [Online]. Available: https://www.easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems-regulations-eu

[19] (2024). *Annex 10—Aeronautical Telecommunications—Volume I—Radio Navigational Aids*. [Online]. Available: https://store.icao.int/en/annex-10-aeronautical-telecommunications-volume-i-radio-navigational-aids

[20] R. Morales-Ferre, P. Richter, E. Falletti, A. De La Fuente, and E. S. Lohan, "A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 249–291, 1st Quart., 2020.

[21] P.-Y. Kong, "A survey of cyberattack countermeasures for unmanned aerial vehicles," *IEEE Access*, vol. 9, pp. 148244–148263, 2021.

[22] A. Rugo, C. A. Ardagna, and N. E. Ioini, "A security review in the UAVNet era: Threats, countermeasures, and gap analysis," *ACM Comput. Surveys*, vol. 55, no. 1, pp. 1–35, Jan. 2023.

[23] N. Gyagenda, J. V. Hatilima, H. Roth, and V. Zhmud, "A review of GNSS-independent UAV navigation techniques," *Robot. Auto. Syst.*, vol. 152, Jun. 2022, Art. no. 104069.

[24] H. J. Hadi, Y. Cao, K. U. Nisa, A. M. Jamil, and Q. Ni, "A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs," *J. Netw. Comput. Appl.*, vol. 213, Apr. 2023, Art. no. 103607.

[25] A. Oracevic and A. Salman, "Unmanned aerial vehicles in peril: Investigating and addressing cyber threats to UAVs," in *Proc. Int. Conf. Smart Appl., Commun. Netw. (SmartNets)*, May 2024, pp. 1–7.

[26] J. Burbank, T. Greene, and N. Kaabouch, "Detecting and mitigating attacks on GPS devices," *Sensors*, vol. 24, no. 17, p. 5529, Aug. 2024.

[27] X. Wang et al., "A survey on security of UAV swarm networks: Attacks and countermeasures," *ACM Comput. Surv.*, vol. 57, no. 3, pp. 1–37, Nov. 2024, doi: 10.1145/3703625.

[28] X. Wei, J. Ma, and C. Sun, "A survey on security of unmanned aerial vehicle systems: Attacks and countermeasures," *IEEE Internet Things J.*, vol. 11, no. 21, pp. 34826–34847, Nov. 2024.

[29] R. Morshedi and S. Mojtaba Matinkhah, "Cybersecurity challenges and solutions in unmanned aerial vehicles (UAVs)," *J. Field Robot.*, vol. 43, no. 1, pp. 314–329, Jan. 2026.

[30] A. Malik and M. Rao, "Radio frequency interference, its mitigation and its implications for the civil aviation industry," *Electronics*, vol. 14, no. 12, p. 2483, Jun. 2025.

[31] P. Jiang et al., "GNSS anti-interference technologies for unmanned systems: A brief review," *Drones*, vol. 9, no. 5, p. 349, May 2025. [Online]. Available: https://www.mdpi.com/2504-446X/9/5/349

[32] E. Aldao, L. González-De Santos, and H. González-Jorge, "LiDAR based detect and avoid system for UAV navigation in UAM corridors," *Drones*, vol. 6, no. 8, p. 185, Jul. 2022.

[33] H. Zhong, Y. Wang, Z. Miao, L. Li, S. Fan, and H. Zhang, "A homography-based visual servo control approach for an underactuated unmanned aerial vehicle in GPS-denied environments," *IEEE Trans. Intell. Vehicles*, vol. 8, no. 2, pp. 1119–1129, Feb. 2023.

[34] U. G. Sefercik and M. Nazar, "Consistency analysis of RTK and non-RTK UAV DSMs in vegetated areas," *IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens.*, vol. 16, pp. 5759–5768, 2023.

[35] D. Medina, J. Vilà-Valls, A. Hesselbarth, R. Ziebold, and J. García, "On the recursive joint position and attitude determination in multi-antenna GNSS platforms," *Remote Sens.*, vol. 12, no. 12, p. 1955, Jun. 2020.

[36] D. Prochniewicz, K. Wezka, and J. Kozuchowska, "Empirical stochastic model of multi-GNSS measurements," *Sensors*, vol. 21, no. 13, p. 4566, Jul. 2021.

[37] M. Wu, J. Li, S. Luo, and W. Liu, "Attitude determination with GPS L1/Galileo E1 observations from common-clock receiver: A comparison of four different models," *Remote Sens.*, vol. 14, no. 21, p. 5438, Oct. 2022.

[38] Y. Shu, P. Xu, X. Niu, Q. Chen, L. Qiao, and J. Liu, "High-rate attitude determination of moving vehicles with GNSS: GPS, BDS, GLONASS, and Galileo," *IEEE Trans. Instrum. Meas.*, vol. 71, pp. 1–13, 2022.

[39] J. K. Holmes, *Spread Spectrum Systems for GNSS and Wireless Communications*. Norwood, MA, USA: Artech House, 2007.

[40] I. Lapin, J. Samson, S. Wallner, C. Lopez, and M. Mabilleau, "Distribution of clock correction and ephemeris parameters in broadcast navigation messages," *GPS Solutions*, vol. 25, no. 3, p. 111, Jul. 2021.

[41] A. Al-Hourani and I. Guvenc, "On modeling satellite-to-ground path-loss in urban environments," *IEEE Commun. Lett.*, vol. 25, no. 3, pp. 696–700, Mar. 2021.

[42] F. Van Graas, A. Soloviev, M. U. De Haag, and S. Gunawardena, "Closed-loop sequential signal processing and open-loop batch processing approaches for GNSS receiver design," *IEEE J. Sel. Topics Signal Process.*, vol. 3, no. 4, pp. 571–586, Aug. 2009.

[43] F. Gao and H. Xia, "Fast GNSS signal acquisition with Doppler frequency estimation algorithm," *GPS solutions*, vol. 22, pp. 1–13, Mar. 2018.

[44] P. J. G. Teunissen, "Integer least-squares theory for the GNSS compass," *J. Geodesy*, vol. 84, no. 7, pp. 433–447, Jul. 2010.

[45] G. Zhang and L.-T. Hsu, "Intelligent GNSS/INS integrated navigation system for a commercial UAV flight control system," *Aerosp. Sci. Technol.*, vol. 80, pp. 368–380, Sep. 2018.

[46] R. Ferreira, J. Gaspar, P. Sebastião, and N. Souto, "A software defined radio based anti-UAV mobile system with jamming and spoofing capabilities," *Sensors*, vol. 22, no. 4, p. 1487, Feb. 2022.

[47] D. Hambling. *Ukraine Will Spoof GPS Across the Country to Stop Russian Drones*. Accessed: Feb. 19, 2025. [Online]. Available: https://www.newscientist.com/article/2415318-ukraine-will-spoof-gps-across-the-country-to-stop-russian-drones/

[48] C. McFadden. *Russian Jammers Plaguing Pilots Near Baltic, 1600 Aircraft Impacted*. Accessed: Feb. 19, 2025. [Online]. Available: https://interestingengineering.com/military/russian-jammers-plaguing-pilots- near-baltic-1600-aircraft-impacted

[49] G. Tian, J. Zhou, X. Li, and D. Li, "Comprehensive experimental research on complex electromagnetic environment of aircraft," *J. Physics: Conf. Ser.*, vol. 1601, no. 2, Jul. 2020, Art. no. 022043.

[50] *RTCA Home*. Accessed: Feb. 15, 2025. [Online]. Available: https://products.rtca.org/

[51] General Requirements for the Flight Control and Navigation System of Small and Light Multi-Rotor Unmanned Aircraft, GB/T Standard 38997-2020, 2020. [Online]. Available: https://www.antpedia.com/standard/1076337685.html

[52] Electromagnetic Compatibility Requirements and Test Methods for Civil Small and Light Unmanned Aircraft System, GB/T Standard 38909-2020, 2020. [Online]. Available: https://www.antpedia.com/standard/1139289045.html

[53] Y. Zidane, J. S. Silva, and G. Tavares, "Jamming and spoofing techniques for drone neutralization: An experimental study," *Drones*, vol. 8, no. 12, p. 743, Dec. 2024.

[54] Z. Zhang, Y. Zhou, Y. Zhang, and B. Qian, "Strong electromagnetic interference and protection in UAVs," *Electronics*, vol. 13, no. 2, p. 393, Jan. 2024.

[55] O. Ceviz, S. Sen, and P. Sadioglu, "A survey of security in UAVs and FANETs: Issues, threats, analysis of attacks, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 27, no. 5, pp. 3227–3265, Oct. 2025.

[56] V. Chamola, P. Kotesh, A. Agarwal, Naren, N. Gupta, and M. Guizani, "A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques," *Ad Hoc Netw.*, vol. 111, Feb. 2021, Art. no. 102324.

[57] Z. Qinglong, C. Erwei, W. Yuming, C. Yazhou, and M. Liyun, "Research on the electromagnetic interference effect of UAV satellite navigation system," *Syst. Eng. Electron.*, vol. 42, no. 12, p. 2684, 2020.

[58] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and privacy issues of UAV: A survey," *Mobile Netw. Appl.*, vol. 25, no. 1, pp. 95–101, Feb. 2020, doi: 10.1007/s11036-018-1193-x.

[59] X. Ma, M. Gao, Y. Zhao, and M. Yu, "A novel navigation spoofing algorithm for UAV based on GPS/INS-integrated navigation," *IEEE Trans. Veh. Technol.*, vol. 73, no. 10, pp. 15424–15439, Oct. 2024.

[60] S. Liaquat, M. Faizan, J. N. Chattha, F. A. Butt, N. M. Mahyuddin, and I. H. Naqvi, "A framework for preventing unauthorized drone intrusions through radar detection and GPS spoofing," *Ain Shams Eng. J.*, vol. 15, no. 5, May 2024, Art. no. 102707.

[61] A. Altaweel, H. Mukkath, and I. Kamel, "GPS spoofing attacks in FANETs: A systematic literature review," *IEEE Access*, vol. 11, pp. 55233–55280, 2023.

[62] S. Z. Khan, M. Mohsin, and W. Iqbal, "On GPS spoofing of aerial platforms: A review of threats, challenges, methodologies, and future research directions," *PeerJ Comput. Sci.*, vol. 7, p. e507, May 2021.

[63] M. Park, B. Shin, J.-H. Han, H.-D. Kim, and C. Kee, "Global navigation satellite system signal generation method for wide area protection against numerous unintentional drones," *IEEE Access*, vol. 9, pp. 154752–154765, 2021.

[64] C. Ma, J. Yang, J. Chen, Z. Qu, and C. Zhou, "Effects of a navigation spoofing signal on a receiver loop and a UAV spoofing approach," *GPS Solutions*, vol. 24, no. 3, pp. 1–13, Jul. 2020.

[65] J. Noh et al., "Tractor beam: Safe-hijacking of consumer drones with adaptive GPS spoofing," *ACM Trans. Privacy Secur.*, vol. 22, no. 2, pp. 1–26, May 2019.

[66] H. Wang, G. Ding, J. Chen, Y. Zou, and F. Gao, "UAV anti-jamming communications with power and mobility control," *IEEE Trans. Wireless Commun.*, vol. 22, no. 7, pp. 4729–4744, Jul. 2023.

[67] J. Jang, M. Paonni, and B. Eissfeller, "CW interference effects on tracking performance of GNSS receivers," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 48, no. 1, pp. 243–258, Jan. 2012.

[68] X. Li et al., "Overview of jamming technology for satellite navigation," *Machines*, vol. 11, no. 7, p. 768, Jul. 2023.

[69] Q. Lv and H. Qin, "A novel algorithm for adaptive notch filter to detect and mitigate the CWI for GNSS receivers," in *Proc. IEEE 3rd Int. Conf. Signal Image Process. (ICSIP)*, Jul. 2018, pp. 444–451.

[70] S. Li, Y. Li, L. Li, and C. Gao, "Exploring the effects of single-tone jamming and multi-tone jamming on B2a signal quality," in *Proc. 3rd Int. Academic Exchange Conf. Sci. Technol. Innov. (IAECST)*, Dec. 2021, pp. 120–123.

[71] G. Novella, A. Garcia-Pena, and C. Macabiau, "C/N0 degradation in presence of chirp interference: Theoretical model," *GPS Solutions*, vol. 28, no. 4, p. 161, Oct. 2024.

[72] Q. Zhou, Y. Li, and Y. Niu, "A countermeasure against random pulse jamming in time domain based on reinforcement learning," *IEEE Access*, vol. 8, pp. 97164–97174, 2020.

[73] N. G. Ferrara, M. Z. H. Bhuiyan, S. Söderholm, L. Ruotsalainen, and H. Kuusniemi, "A new implementation of narrowband interference detection, characterization, and mitigation technique for a software-defined multi-GNSS receiver," *GPS Solutions*, vol. 22, no. 4, pp. 1–15, Oct. 2018.

[74] M. Ding, W. Chen, and W. Ding, "Performance analysis of a normal GNSS receiver model under different types of jamming signals," *Measurement*, vol. 214, Jun. 2023, Art. no. 112786.

[75] D. Borio, F. Dovis, H. Kuusniemi, and L. Lo Presti, "Impact and detection of GNSS jammers on consumer grade satellite navigation receivers," *Proc. IEEE*, vol. 104, no. 6, pp. 1233–1245, Jun. 2016.

[76] A. Garcia-Pena, G. Novella, and C. Macabiau, "C/N0 degradation in presence of chirp interference: Statistical, real and estimated C/N0," *GPS Solutions*, vol. 28, no. 4, p. 197, Oct. 2024.

[77] A. Garcia-Pena, O. Julien, C. Macabiau, M. Mabilleau, and P. Durel, "GNSS C/N0 degradation model in presence of continuous wave and pulsed interference," *NAVIGATION, J. Inst. Navigat.*, vol. 68, no. 1, pp. 75–91, Mar. 2021.

[78] W. Feng, J.-M. Friedt, G. Goavec-Merou, and F. Meyer, "Software-defined radio implemented GPS spoofing and its computationally efficient detection and suppression," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 36, no. 3, pp. 36–52, Mar. 2021.

[79] J. R. V. D. Merwe, X. Zubizarreta, I. Lukcin, A. Rügamer, and W. Felber, "Classification of spoofing attack types," in *Proc. Eur. Navigat. Conf. (ENC)*, May 2018, pp. 91–99.

[80] L. Junzhi, L. Wanqing, F. Qixiang, and L. Beidian, "Research progress of GNSS spoofing and spoofing detection technology," in *Proc. IEEE 19th Int. Conf. Commun. Technol. (ICCT)*, Oct. 2019, pp. 1360–1369.

[81] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.

[82] X. Li et al., "Tradeoff of code estimation error rate and terminal gain in SCER attack," *IEEE Trans. Instrum. Meas.*, vol. 73, pp. 1–12, 2024.

[83] M. S. Kumar, G. S. Kasbekar, and A. Maity, "Identification of GPS spoofing as a drone cyber-vulnerability and evaluation of efficacy of asynchronous GPS spoofing," *IFAC-PapersOnLine*, vol. 55, no. 22, pp. 394–399, 2022.

[84] Y. Wang, Y. Kou, and Z. Huang, "Necessary condition for the success of synchronous GNSS spoofing," *Chin. J. Electron.*, vol. 32, no. 3, pp. 438–452, May 2023.

[85] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proc. 18th ACM Conf. Comput. Commun. Secur.*, Oct. 2011, pp. 75–86.

[86] J. Chang, F. Huang, L. Zhang, D. Xu, and L.-T. Hsu, "Selection of areas for effective GNSS spoofing attacks to a vehicle-mounted MSF system based on scenario classification models," *IEEE Trans. Veh. Technol.*, vol. 72, no. 11, pp. 14645–14655, Nov. 2023.

[87] D. He, G. Yang, H. Li, S. Chan, Y. Cheng, and N. Guizani, "An effective countermeasure against UAV swarm attack," *IEEE Netw.*, vol. 35, no. 1, pp. 380–385, Jan. 2021.

[88] M. Ceccato, F. Formaggio, and S. Tomasin, "Spatial GNSS spoofing against drone swarms with multiple antennas and Wiener filter," *IEEE Trans. Signal Process.*, vol. 68, pp. 5782–5794, 2020.

[89] X. Ma and M. Gao, "'Lure the enemy in deep': Confronting rogue UAV through diverse hybrid jamming," *IEEE Access*, vol. 13, pp. 68351–68369, 2025.

[90] Y. Gao and G. Li, "A GNSS instrumentation covert directional spoofing algorithm for UAV equipped with tightly-coupled GNSS/IMU," *IEEE Trans. Instrum. Meas.*, vol. 72, pp. 1–13, 2023.

[91] X. Geng, Y. Guo, K. Tang, W. Wu, Y. Ren, and G. Duan, "A covert spoofing algorithm for SINS/GNSS tightly integrated navigation system," *IEEE Trans. Autom. Sci. Eng.*, vol. 22, pp. 6134–6142, 2025.

[92] H. Chen, Z. Wen, and C. Lei, "Optimization of covert spoofing parameters for loosely coupled GNSS/INS systems based on improved genetic algorithm," *Sci. Rep.*, vol. 15, no. 1, p. 7285, Mar. 2025.

[93] J. H. Jung, M. Y. Hong, and J. W. Yoon, "GPS spoofing attacks on autonomous navigation systems for UAVs," *IEEE Access*, vol. 13, pp. 178821–178833, 2025.

[94] X. Geng, Y. Guo, K. Tang, W. Wu, and Y. Ren, "Research on covert directional spoofing method for INS/GNSS loosely integrated navigation," *IEEE Trans. Veh. Technol.*, vol. 72, no. 5, pp. 5654–5663, May 2023.

[95] C. Tang, X. Zhou, L. Zhang, Y. Liu, and Z. Dan, "LEO satellite navigation signal multi-dimensional interference optimisation method based on hybrid game theory," *Remote Sens.*, vol. 17, no. 8, p. 1444, Apr. 2025. [Online]. Available: https://www.mdpi.com/2072-4292/17/8/1444

[96] X. Geng, K. Tang, Y. Guo, L. Zhang, W. Wu, and T. Ma, "A distributed UAV swarm countermeasure method based on GNSS spoofing," *IEEE Internet Things J.*, vol. 12, no. 16, pp. 33455–33467, Aug. 2025.

[97] X. Ma, T. Sun, and M. Gao, "A reinforcement-learning-enhanced spoofing algorithm for UAV with GPS/INS-integrated navigation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 61, no. 4, pp. 8659–8673, Aug. 2025.

[98] M. Alkhatib, M. Nayfeh, K. Al Shamaileh, N. Kaabouch, and V. Devabhaktuni, "A return-to-home unmanned aerial vehicle navigation solution in global positioning system denied environments via bidirectional long short-term memory reverse flightpath prediction," *Eng. Appl. Artif. Intell.*, vol. 140, Jan. 2025, Art. no. 109729.

[99] G. Corraro, I. Iudice, G. Cuciniello, U. Ciniglio, and D. Pascarella, "GNSS threat simulator for urban air mobility scenarios," *Aerospace*, vol. 12, no. 9, p. 787, Aug. 2025.

[100] Z. Wu, C. Liang, and Y. Zhang, "Blockchain-based authentication of GNSS civil navigation message," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 59, no. 4, pp. 4380–4392, Aug. 2023.

[101] G. Michieletto, F. Formaggio, A. Cenedese, and S. Tomasin, "Robust localization for secure navigation of UAV formations under GNSS spoofing attack," *IEEE Trans. Autom. Sci. Eng.*, vol. 20, no. 4, pp. 2383–2396, Oct. 2023.

[102] I. GNSS. (Nov. 2020). *Anti-Jam GPS for Army's Gray Eagle UAV Awarded to Cobham*. [Online]. Available: https://insidegnss.com/anti-jam-gps-for-armys-gray-eagle-uav-awarded-to-cobham/

[103] S. Bang and J. Kim, "Adaptive switching strategy of an aerial drone's GNSS antennas with metallic shielding for GNSS anti-jamming," *Sensors*, vol. 25, no. 18, p. 5778, Sep. 2025.

[104] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simon, I. Rodríguez, and J. D. Calle, "A navigation message authentication proposal for the Galileo open service," *Navigation*, vol. 63, no. 1, pp. 85–102, Mar. 2016.

[105] U. S. G. A. Office. *GPS Modernization: DOD Continuing to Develop New Jam-Resistant Capability, But Widespread Use Remains Years Away — U.S. GAO*. Accessed: Mar. 20, 2025. [Online]. Available: https://www.gao.gov/products/gao-21-145

[106] O. K. Isik, I. Petrunin, and A. Tsourdos, "Machine learning-based environment-aware GNSS integrity monitoring for urban air mobility," *Drones*, vol. 8, no. 11, p. 690, Nov. 2024.

[107] N. Spens, D.-K. Lee, and D. Akos, "An application for detecting GNSS jamming and spoofing," in *Proc. 33rd Int. Tech. Meeting Satellite Division Inst. Navig. (ION GNSS+)*, Sep. 2021, pp. 1981–1988.

[108] P. Wang, E. Cetin, A. G. Dempster, Y. Wang, and S. Wu, "GNSS interference detection using statistical analysis in the time-frequency domain," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 54, no. 1, pp. 416–428, Feb. 2018.

[109] K. Sun, M. Zhang, and D. Yang, "A new interference detection method based on joint hybrid time–frequency distribution for GNSS receivers," *IEEE Trans. Veh. Technol.*, vol. 65, no. 11, pp. 9057–9071, Nov. 2016.

[110] F. B. Da Silva, E. Cetin, and W. A. Martins, "Radio frequency interference detection using nonnegative matrix factorization," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 2, pp. 868–878, Apr. 2022.

[111] M. Spanghero, F. Geib, R. Panier, and P. Papadimitratos, "GNSS jammer localization and identification with airborne commercial GNSS receivers," *IEEE Trans. Inf. Forensics Security*, vol. 20, pp. 3550–3565, 2025.

[112] Y. Yang, Z. Peng, W. Zhang, and G. Meng, "Parameterised time-frequency analysis methods and their engineering applications: A review of recent advances," *Mech. Syst. Signal Process.*, vol. 119, pp. 182–221, Mar. 2019.

[113] E. Axell, F. M. Eklöf, P. Johansson, M. Alexandersson, and D. M. Akos, "Jamming detection in GNSS receivers: Performance evaluation of field trials," *Navigation*, vol. 62, no. 1, pp. 73–82, Mar. 2015.

[114] C. Sakorn and P. Supnithi, "Calculating AGC and C/N0 thresholds of mobile for jamming detection," in *Proc. 18th Int. Conf. Electr. Engineering/Electronics, Comput., Telecommun. Inf. Technol. (ECTI-CON)*, May 2021, pp. 268–271.

[115] J. Arribas, C. Fernandez-Prades, and P. Closas, "Antenna array based GNSS signal acquisition for interference mitigation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 1, pp. 223–243, Jan. 2013.

[116] A. Osman, M. M. E. Moussa, M. Tamazin, M. J. Korenberg, and A. Noureldin, "DOA elevation and azimuth angles estimation of GPS jamming signals using fast orthogonal search," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 5, pp. 3812–3821, Oct. 2020.

[117] M. Moussa, A. Osman, M. Tamazin, M. J. Korenberg, and A. Noureldin, "Direction of arrival estimation of GPS narrowband jammers using high-resolution techniques," *Sensors*, vol. 19, no. 24, p. 5532, Dec. 2019.

[118] O. Sharifi-Tehrani, M. F. Sabahi, and M. R. Danaee, "Low-complexity framework for GNSS jamming and spoofing detection on moving platforms," *IET Radar, Sonar Navigat.*, vol. 14, no. 12, pp. 2027–2038, Dec. 2020.

[119] W. Qin and F. Dovis, "Situational awareness of chirp jamming threats to GNSS based on supervised machine learning," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 3, pp. 1707–1720, Jun. 2022.

[120] M. Alkhatib et al., "Classification and source location indication of jamming attacks targeting UAVs via multi-output multiclass machine learning modeling," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2024, pp. 1–5.

[121] 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 Trans. Aerosp. Electron. Syst.*, vol. 60, no. 3, pp. 2705–2721, Jun. 2024.

[122] R. Morales Ferre, A. De La Fuente, and E. S. Lohan, "Jammer classification in GNSS bands via machine learning algorithms," *Sensors*, vol. 19, no. 22, p. 4841, Nov. 2019.

[123] J. Sormayli, M. Darvishi, K. Zarrinnegar, and M. R. Mosavi, "Real-time jamming detection using windowing and hybrid machine learning models for pre-saturation alerts," *Sci. Rep.*, vol. 15, no. 1, p. 24748, Jul. 2025, doi: 10.1038/s41598-025-10567-0.

[124] I. E. Mehr and F. Dovis, "A deep neural network approach for classification of GNSS interference and jamming," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 61, no. 2, pp. 1660–1676, Apr. 2025.

[125] X. Chen, D. He, X. Yan, W. Yu, and T.-K. Truong, "GNSS interference type recognition with fingerprint spectrum DNN method," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 5, pp. 4745–4760, Oct. 2022.

[126] A. Reda and T. Mekkawy, "GNSS jamming detection using attention-based mutual information feature selection," *Discover Appl. Sci.*, vol. 6, no. 4, p. 163, Mar. 2024.

[127] S. Li, X. Tang, H. Lin, and F. Wang, "GNSS spoofing detection based on frequency domain processing," *Measurement*, vol. 242, Jan. 2025, Art. no. 115872.

[128] J. Fang, J. Yue, B. Xu, and L.-T. Hsu, "A post-correlation graphical way for continuous GNSS spoofing detection," *Measurement*, vol. 216, Jul. 2023, Art. no. 112974.

[129] Y. Wang, Y. Kou, Y. Zhao, and Z. Huang, "Detection of synchronous spoofing on a GNSS receiver using weighed double ratio metrics," *GPS Solutions*, vol. 26, no. 3, p. 91, Jul. 2022.

[130] L. Zhang, L. Wang, R. Wu, and X. Zhuang, "A new approach for GNSS spoofing detection using power and signal quality monitoring," *Meas. Sci. Technol.*, vol. 35, no. 12, Dec. 2024, Art. no. 126109.

[131] 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 Trans. Instrum. Meas.*, vol. 70, pp. 1–15, 2021.

[132] J. Li et al., "A real-time GNSS time spoofing detection framework based on feature processing," *GPS Solutions*, vol. 29, no. 1, p. 45, Jan. 2025.

[133] X. Wei, C. Sun, X. Li, and J. Ma, "GNSS spoofing detection for UAVs using Doppler frequency and carrier-to-noise density ratio," *J. Syst. Archit.*, vol. 153, Aug. 2024, Art. no. 103212.

[134] X. Zhu, Z. Lu, T. Hua, F. Yang, G. Tu, and X. Chen, "A novel GPS meaconing spoofing detection technique based on improved ratio combined with carrier-to-noise moving variance," *Electronics*, vol. 11, no. 5, p. 738, Feb. 2022.

[135] S. Lo, F. Rothmaier, D. Miralles, D. Akos, and T. Walter, "Developing a practical GNSS spoofing detection thresholds for receiver power monitoring," in *Proc. I_{ON} GNSS+, Int. Tech. Meeting Satell. Division Inst. Navigat.*, Oct. 2021, pp. 803–815.

[136] E. G. Manfredini, D. M. Akos, Y.-H. Chen, S. Lo, T. Walter, and P. Enge, "Effective GPS spoofing detection utilizing metrics from commercial receivers," in *Proc. Int. Tech. Meeting The Inst. Navigat.*, Feb. 2018, pp. 672–689.

[137] W. Wang, I. Aguilar Sanchez, G. Caparra, A. McKeown, T. Whitworth, and E. S. Lohan, "A survey of spoofer detection techniques via radio frequency fingerprinting with focus on the GNSS pre-correlation sampled data," *Sensors*, vol. 21, no. 9, p. 3012, Apr. 2021.

[138] R. Morales-Ferre, W. Wang, A. Sanz-Abia, and E.-S. Lohan, "Identifying GNSS signals based on their radio frequency (RF) features—A dataset with GNSS raw signals based on roof antennas and spectracom generator," *Data*, vol. 5, no. 1, p. 18, Feb. 2020.

[139] C. Guo and Z. Yang, "A robust RF fingerprint extraction scheme for GNSS spoofing detection," in *Proc. I_{ON} GNSS+, Int. Tech. Meeting Satell. Division Inst. Navigat.*, Oct. 2023, pp. 199–205.

[140] X. Zhang, Y. Huang, Y. Tian, M. Lin, and J. An, "Noise-like features-assisted GNSS spoofing detection based on convolutional autoencoder," *IEEE Sensors J.*, vol. 23, no. 20, pp. 25473–25486, Oct. 2023.

[141] W. Wang, E. S. Lohan, I. A. Sanchez, and G. Caparra, "Pre-correlation and post-correlation RF fingerprinting methods for GNSS spoofer identification with real-field measurement data," in *Proc. 10th Workshop Satell. Navigat. Technol. (NAVITEC)*, Apr. 2022, pp. 1–10.

[142] L. Xiao, X. Li, and G. Wang, "GNSS spoofing detection using pseudorange double differences between two receivers," in *Proc. IEEE 7th Int. Conf. Comput. Sci. Netw. Technol. (ICCSNT)*, Oct. 2019, pp. 498–502.

[143] J. Wen, H. Li, and M. Lu, "A flexible GNSS spoofer localization system: Spoofing discrimination and localization method," *NAVIGATION, J. Inst. Navigat.*, vol. 69, no. 1, 2022, Art. no. navi.511.

[144] X. Shang, F. Sun, L. Zhang, J. Cui, and Y. Zhang, "Detection and mitigation of GNSS spoofing via the pseudorange difference between epochs in a multicorrelator receiver," *GPS Solutions*, vol. 26, no. 2, p. 37, Apr. 2022.

[145] S.-H. Seo, B.-H. Lee, S.-H. Im, G.-I. Jee, and K.-S. Kim, "Efficient spoofing identification using baseline vector information of multiple receivers," *GPS Solutions*, vol. 22, no. 4, p. 115, Oct. 2018.

[146] V. Truong, A. Vervisch-Picois, J. Rubio Hernan, and N. Samama, "Characterization of the ability of low-cost GNSS receiver to detect spoofing using clock bias," *Sensors*, vol. 23, no. 5, p. 2735, Mar. 2023.

[147] F. Feng, X. Li, W. Wei, Y. Si, and X. Zhu, "A GNSS time synchronization attack detection method for commercial off-the-shelf receivers: Cumulative second-order difference of pseudoranges," *IEEE Internet Things J.*, vol. 12, no. 3, pp. 2322–2333, Feb. 2025.

[148] M. C. Esswein and M. L. Psiaki, "Classification of authentic and spoofed GNSS signals using a calibrated antenna array," *NAVIGATION, J. Inst. Navigat.*, vol. 72, no. 1, Jan. 2025, Art. no. navi.675.

[149] R. Liu, Z. Yang, Q. Chen, G. Liao, and Q. Zhu, "Localization of GNSS spoofing interference source based on a moving array antenna," *Remote Sens.*, vol. 15, no. 23, p. 5497, Nov. 2023.

[150] Y. Zhao, F. Shen, D. Xu, and Z. Meng, "A coprime array-based technique for spoofing detection and DOA estimation in GNSS," *IEEE Sensors J.*, vol. 22, no. 23, pp. 22828–22835, Dec. 2022.

[151] J. Chen, X. Wang, Z. Fang, C. Jiang, M. Gao, and Y. Xu, "A real-time spoofing detection method using three low-cost antennas in satellite navigation," *Electronics*, vol. 13, no. 6, p. 1134, Mar. 2024.

[152] J. Chen, Y. Xu, H. Yuan, and Y. Yuan, "A new GNSS spoofing detection method using two antennas," *IEEE Access*, vol. 8, pp. 110738–110747, 2020.

[153] M. Nayfeh, Y. Li, K. A. Shamaileh, V. Devabhaktuni, and N. Kaabouch, "Machine learning modeling of GPS features with applications to UAV location spoofing detection and classification," *Comput. Secur.*, vol. 126, Mar. 2023, Art. no. 103085.

[154] T. T. Khoei, A. Gasimova, M. A. Ahajjam, K. A. Shamaileh, V. Devabhaktuni, and N. Kaabouch, "A comparative analysis of supervised and unsupervised models for detecting GPS spoofing attack on UAVs," in *Proc. IEEE Int. Conf. Electro Inf. Technol. (eIT)*, May 2022, pp. 279–284.

[155] G. Aissou, H. O. Slimane, S. Benouadah, and N. Kaabouch, "Tree-based supervised machine learning models for detecting GPS spoofing attacks on UAS," in *Proc. IEEE 12th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Dec. 2021, pp. 0649–0653.

[156] Z. Chen, J. Li, J. Li, X. Zhu, and C. Li, "GNSS multiparameter spoofing detection method based on support vector machine," *IEEE Sensors J.*, vol. 22, no. 18, pp. 17864–17874, Sep. 2022.

[157] J. Li, X. Zhu, M. Ouyang, W. Li, Z. Chen, and Q. Fu, "GNSS spoofing jamming detection based on generative adversarial network," *IEEE Sensors J.*, vol. 21, no. 20, pp. 22823–22832, Oct. 2021.

[158] W. Mao, J. Ren, and S. Ni, "Fast GNSS spoofing detection based on LSTM-detect model," *GPS Solutions*, vol. 29, no. 1, pp. 1–17, Jan. 2025.

[159] M. S. Korium, M. Saber, A. M. Ahmed, A. Narayanan, and P. H. J. Nardelli, "Image-based intrusion detection system for GPS spoofing cyberattacks in unmanned aerial vehicles," *Ad Hoc Netw.*, vol. 163, Oct. 2024, Art. no. 103597.

[160] Y. Sun, M. Yu, L. Wang, T. Li, and M. Dong, "A deep-learning-based GPS signal spoofing detection method for small UAVs," *Drones*, vol. 7, no. 6, p. 370, Jun. 2023.

[161] Z. Feng et al., "An efficient UAV hijacking detection method using onboard inertial measurement unit," *ACM Trans. Embedded Comput. Syst.*, vol. 17, no. 6, pp. 1–19, Nov. 2018.

[162] Z. Feng et al., "Efficient drone hijacking detection using two-step GA-XGBoost," *J. Syst. Archit.*, vol. 103, Feb. 2020, Art. no. 101694.

[163] X. Jin, X. Zhang, S. Li, and S. Zheng, "Detection of slowly varying spoofing using weighted Kalman gain in GNSS/INS tightly coupled systems," *GPS Solutions*, vol. 28, no. 1, p. 54, Jan. 2024.

[164] A. V. Savkin, W. Ni, and M. Eskandari, "Effective UAV navigation for cellular-assisted radio sensing, imaging, and tracking," *IEEE Trans. Veh. Technol.*, vol. 72, no. 10, pp. 13729–13733, Oct. 2023.

[165] L. Bai, C. Sun, A. G. Dempster, H. Zhao, and W. Feng, "GNSS spoofing detection and mitigation with a single 5G base station aiding," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 60, no. 4, pp. 4601–4620, Aug. 2024.

[166] Y. Dang, C. Benzaïd, B. Yang, T. Taleb, and Y. Shen, "Deep-ensemble-learning-based GPS spoofing detection for cellular-connected UAVs," *IEEE Internet Things J.*, vol. 9, no. 24, pp. 25068–25085, Dec. 2022.

[167] B. Davidovich, B. Nassi, and Y. Elovici, "Towards the detection of GPS spoofing attacks against drones by analyzing camera's video stream," *Sensors*, vol. 22, no. 7, p. 2608, Mar. 2022.

[168] J. Wang, L. Nie, Z. Gu, and H. Zhao, "Real-time detection for GPS spoofing of quad-rotor helicopter based on data fusion," in *Proc. Int. Conf. Intell. Comput.*, 2024, pp. 294–305.

[169] M. Y. Arafat, M. M. Alam, and S. Moh, "Vision-based navigation techniques for unmanned aerial vehicles: Review and challenges," *Drones*, vol. 7, no. 2, p. 89, Jan. 2023.

[170] A. L. Kintz and I. J. Gupta, "A modified MUSIC algorithm for direction of arrival estimation in the presence of antenna array manifold mismatch," *IEEE Trans. Antennas Propag.*, vol. 64, no. 11, pp. 4836–4847, Nov. 2016.

[171] M. M. N. Zanjani and S. H. Sedighy, "Hybrid CNN architectures for detecting and classification of GNSS jamming attacks," *GPS Solutions*, vol. 29, no. 3, p. 115, Jul. 2025.

[172] W. Zhong, H. Xiong, Y. Hua, D. H. Shah, Z. Liao, and Y. Xu, "TSFANet: Temporal–spatial feature aggregation network for GNSS jamming recognition," *IEEE Trans. Instrum. Meas.*, vol. 73, pp. 1–13, 2024.

[173] A. Reda, T. Mekkawy, T. A. Tsiftsis, and A. Mahran, "Deep learning approach for GNSS jamming detection-based PCA and Bayesian optimization feature selection algorithm," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 60, no. 6, pp. 8349–8363, Dec. 2024.

[174] Y. Chai, M. Liu, and M. Li, "Navigation spoofing and jamming signals identification of UAV based on federated learning," *IEEE Internet Things J.*, vol. 12, no. 21, pp. 44177–44188, Nov. 2025.

[175] X. Wei, Y. Wang, and C. Sun, "PerDet: Machine-learning-based UAV GPS spoofing detection using perception data," *Remote Sens.*, vol. 14, no. 19, p. 4925, Oct. 2022.

[176] P. Sun, H. Xiong, D. H. Shah, Y. Liu, and B. Zhou, "Multiparameter joint GNSS spoofing detection based on TSVAE," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 61, no. 2, pp. 3373–3386, Apr. 2025.

[177] S.-Q. Wang, J. Liu, B.-G. Cai, J. Wang, and D.-B. Lu, "Multidomain joint spoofing detection based on a semi-supervised detection network for GNSS-based train positioning," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 61, no. 2, pp. 3936–3949, Apr. 2025.

[178] D. She, W. Wang, Z. Yin, J. Wang, and H. Shan, "GPS spoofing attack recognition for UAVs with limited samples," *IEEE Internet Things J.*, vol. 12, no. 1, pp. 250–261, Jan. 2025.

[179] W. Zhou, Z. Lv, G. Li, B. Jiao, and W. Wu, "Detection of spoofing attacks on global navigation satellite systems using Kolmogorov–Smirnov test-based signal quality monitoring method," *IEEE Sensors J.*, vol. 24, no. 7, pp. 10474–10490, Apr. 2024.

[180] A. Iqbal, M. N. Aman, and B. Sikdar, "A deep learning based induced GNSS spoof detection framework," *IEEE Trans. Mach. Learn. Commun. Netw.*, vol. 2, pp. 457–478, 2024.

[181] D. C. Franco, J. R. Van Der Merwe, and A. Rügamer, "GNSS processed interference features," Fraunhofer Inst. Integr. Circuits IIS, Nuremberg, Germany, Tech. Rep., 2023, doi: 10.21227/xxfh-qp91.

[182] T. E. Humphreys, J. A. Bhatti, D. Shepard, and K. Wesson, "The Texas spoofing test battery: Toward a standard for evaluating GPS signal authentication techniques," Dept. Aerosp. Eng., Radionavigation Lab., Univ. Texas Austin, Austin, TX, USA, Tech. Rep., 2012.

[183] A. Albright, S. Powers, J. Bonior, and F. Combs, "A tool for furthering GNSS security research: The oak ridge spoofing and interference test battery (OAKBAT)," in *Proc. I_{ON} GNSS+, Int. Tech. Meeting Satell. Division Inst. Navigat.*, Oct. 2020, pp. 3697–3712.

[184] J. Whelan, T. Sangarapillai, O. Minawi, A. Almehmadi, and K. El-Khatib, "UAV attack dataset," Ontario Tech Univ., Oshawa, ON, Canada, Tech. Rep., 2020, doi: 10.21227/00dg-0d12.

[185] H. Li, S. Tang, P. Wu, and P. Closas, "Robust interference mitigation techniques for direct position estimation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 59, no. 6, pp. 8969–8980, Dec. 2023.

[186] A. Elango, A. Al-Tahmeesschi, M. Saukkoriipi, T. Malmivirta, and L. Ruotsalainen, "WHITE PAPER: Protecting GNSS against intentional interference," 2022, *arXiv:2208.11555*.

[187] E. Falletti, M. T. Gamba, and M. Pini, "Design and analysis of activation strategies for adaptive notch filters to suppress GNSS jamming," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 5, pp. 3718–3734, Oct. 2020.

[188] W. Qin, M. T. Gamba, E. Falletti, and F. Dovis, "An assessment of impact of adaptive notch filters for interference removal on the signal processing stages of a GNSS receiver," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 5, pp. 4067–4082, Oct. 2020.

[189] D. Borio and C. Gioia, "GNSS interference mitigation: A measurement and position domain assessment," *NAVIGATION*, vol. 68, no. 1, pp. 93–114, Mar. 2021.

[190] D. Borio and C. Gioia, "Interference mitigation: Impact on GNSS timing," *GPS Solutions*, vol. 25, no. 2, p. 37, Apr. 2021.

[191] J. Song, Z. Lu, W. Xiao, C. Li, Y. Wang, and G. Sun, "Power-enhanced GNSS interference mitigation with sensed equivalent bandwidth based on ASF algorithm," *IEEE Sensors J.*, vol. 25, no. 2, pp. 2886–2896, Jan. 2025.

[192] J. R. Van Der Merwe, I. Cortés, F. Garzia, A. Rügamer, and W. Felber, "Multi-parameter adaptive notch filter (MPANF) for enhanced interference mitigation," *NAVIGATION, J. Inst. Navigat.*, vol. 70, no. 2, 2023, Art. no. navi.570.

[193] M. Ding, W. Chen, D. Weng, and X. Mi, "Adaptive jamming mitigation in single-antenna receivers with spectral analysis and switchable filtering," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 60, no. 5, pp. 5891–5905, Oct. 2024.

[194] S. Savasta, L. L. Presti, and M. Rao, "Interference mitigation in GNSS receivers by a time-frequency approach," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 1, pp. 415–438, Jan. 2013.

[195] F. B. Da Silva, E. Cetin, and W. A. Martins, "Radio frequency interference mitigation via nonnegative matrix factorization for GNSS," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 59, no. 4, pp. 3493–3504, Aug. 2023.

[196] J. S. L. Kambham and M. Ramarakula, "An efficient approach for anti-jamming in IRNSS receivers using improved PSO based parametric wavelet packet thresholding," *Satell. Navigat.*, vol. 3, no. 1, p. 21, Oct. 2022.

[197] X. Jiang, M. Lei, Y. Niu, J. Wan, and N. Xia, "An anti-interference method based on energy residual searching in GNSS positioning applications," *Electronics*, vol. 13, no. 23, p. 4713, Nov. 2024.

[198] K. Sun, M. Elhajj, and W. Y. Ochieng, "A GNSS anti-interference method based on fractional Fourier transform," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 60, no. 5, pp. 5636–5650, Oct. 2024.

[199] K. Sun, B. Yu, L. Xu, M. Elhajj, and W. Y. Ochieng, "A novel GNSS anti-interference method using fractional Fourier transform and notch filtering," *IEEE Trans. Instrum. Meas.*, vol. 73, pp. 1–17, 2024.

[200] P. Wang, Y. Wang, E. Cetin, A. G. Dempster, and S. Wu, "Time-frequency jammer mitigation based on Kalman filter for GNSS receivers," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 3, pp. 1561–1567, Jun. 2019.

[201] Y. Luo et al., "Zak-transform-based adaptive interference extraction method for GNSS interference mitigation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 60, no. 4, pp. 4784–4793, Aug. 2024.

[202] K. Sun and Y. Chen, "A novel GNSS sweep interference detection and mitigation method based on radon–wigner transform," *IEEE Sensors J.*, vol. 23, no. 21, pp. 26087–26095, Nov. 2023.

[203] J. Zhang, X. Cui, H. Xu, and M. Lu, "A two-stage interference suppression scheme based on antenna array for GNSS jamming and spoofing," *Sensors*, vol. 19, no. 18, p. 3870, Sep. 2019.

[204] C. Fernández-Prades, J. Arribas, and P. Closas, "Robust GNSS receivers by array signal processing: Theory and implementation," *Proc. IEEE*, vol. 104, no. 6, pp. 1207–1220, Jun. 2016.

[205] R. T. Compton, "The power-inversion adaptive array: Concept and performance," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-15, no. 6, pp. 803–814, Nov. 1979.

[206] H.-W. Chen and J.-W. Zhao, "Wideband MVDR beamforming for acoustic vector sensor linear array," *IEE Proc. - Radar, Sonar Navigat.*, vol. 151, no. 3, pp. 158–162, Jun. 2004.

[207] N. Vagle, A. Broumandan, and G. Lachapelle, "Analysis of multi-antenna GNSS receiver performance under jamming attacks," *Sensors*, vol. 16, no. 11, p. 1937, Nov. 2016.

[208] S. Daneshmand, A. Jahromi, A. Broumandan, and G. Lachapelle, "GNSS space-time interference mitigation and attitude determination in the presence of interference signals," *Sensors*, vol. 15, no. 6, pp. 12180–12204, May 2015.

[209] M. Brachvogel, M. Niestroj, M. Meurer, S. N. Hasnain, R. Stephan, and M. A. Hein, "Space-time adaptive processing as a solution for mitigating interference using spatially-distributed antenna arrays," *NAVIGATION, J. Inst. Navigat.*, vol. 70, no. 3, 2023, Art. no. navi.592.

[210] Z. Lu et al., "Achieving robust and adaptive anti-jamming for GNSS-Receivers based on CPCLMS," *IEEE Trans. Aerosp. Electron. Syst.*, early access, Jan. 12, 2026, doi: 10.1109/TAES.2026.3653343.

[211] K. J. Silva Lorraine and M. Ramarakula, "A comprehensive survey on GNSS interferences and the application of neural networks for anti-jamming," *IETE J. Res.*, vol. 69, no. 7, pp. 4286–4305, Sep. 2023.

[212] D. Li, P. Zhang, J. Zhao, J. Cheng, and H. Zhao, "MP mitigation in GNSS positioning by GRU NNs and adaptive wavelet filtering," *IET Commun.*, vol. 13, no. 17, pp. 2756–2766, Oct. 2019.

[213] J. Sun, Z. Tang, J. Wei, and Y. Ren, "Co-channel interference cancellation method based on deep neural network for LEO satellite systems," in *Proc. China Satell. Navigat. Conf.*, 2021, pp. 270–279.

[214] C.-Z. Wang, L.-W. Kong, J. Jiang, and Y.-C. Lai, "Machine learning-based approach to GPS antijamming," *GPS Solutions*, vol. 25, no. 3, p. 115, Jul. 2021.

[215] Y. Xie, L. Chen, K. Zhang, X. Huang, J. Peng, and S. Ni, "Deep neural network based anti-jamming processing in the GNSS array receiver," *GPS Solutions*, vol. 29, no. 2, p. 63, Apr. 2025.

[216] B. Yang, M. Tian, Y. Ji, J. Cheng, Z. Xie, and S. Shao, "Research on GNSS spoofing mitigation technology based on spoofing correlation peak cancellation," *IEEE Commun. Lett.*, vol. 26, no. 12, pp. 3024–3028, Dec. 2022.

[217] N. Dabaghi Daryan, S. Tohidi, and M. R. Mosavi, "Intelligent mitigation of GPS spoofing using the Kalman filter in the tracking loop based on multi-correlator," *Surv. Rev.*, vol. 57, no. 402, pp. 205–225, May 2025.

[218] Y. Guo, L. Miao, and X. Zhang, "Spoofing detection and mitigation in a multi-correlator GPS receiver based on the maximum likelihood principle," *Sensors*, vol. 19, no. 1, p. 37, Dec. 2018.

[219] N. Stenberg, E. Axell, J. Rantakokko, and G. Hendeby, "Results on GNSS spoofing mitigation using multiple receivers," *NAVIGATION, J. Inst. Navigat.*, vol. 69, no. 1, 2022, Art. no. navi.510.

[220] X. Yan and H. Huang, "Countering spoofing attacks for unmanned aerial vehicles using multi-constellation GNSS," in *Proc. IEEE 18th Int. Conf. Control Autom. (ICCA)*, Jun. 2024, pp. 562–566.

[221] W. Sun, F. Sun, H. Gao, L. Zhang, K. Xiao, and P. Xiao, "Anti-spoofing performance assessment of the vector tracking loop in challenging environments," *IEEE Trans. Instrum. Meas.*, vol. 74, pp. 1–12, 2025.

[222] X. Jin, X. Zhang, S. Xu, S. Li, and S. Zheng, "Robust spoofing detection and mitigation in GNSS using iterative refinement and adaptive filtering," *Chin. J. Aeronaut.*, vol. 38, no. 8, Aug. 2025, Art. no. 103358.

[223] J. Fang and B. Xu, "Spoofing mitigation based on Doppler frequency and pseudorange corrections in GNSS receiver," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Apr. 2025, pp. 306–315.

[224] L. Chen, X. Ouyang, F. Zeng, Y. Ming, and S. Han, "GNSS spoofing mitigation based on code-carrier difference pair pseudorange correction," *IEEE Trans. Instrum. Meas.*, vol. 74, pp. 1–16, 2025.

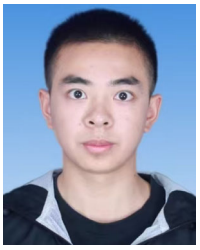
[225] H. Tan, N. Xie, L. Huang, and H. Li, "Enhancing GNSS signal authentication through multi-antenna systems," *IEEE Trans. Wireless Commun.*, vol. 24, no. 5, pp. 4361–4376, May 2025.

[226] J. Magiera, "A multi-antenna scheme for early detection and mitigation of intermediate GNSS spoofing," *Sensors*, vol. 19, no. 10, p. 2411, May 2019.

[227] J. H. Noh, B. H. Gong, Y. S. Lee, B. C. Jung, S. J. Lee, and H. H. Choi, "Performance analysis of GNSS spoofing mitigation techniques based on array antennas in various spoofing scenarios," in *Proc. Int. Tech. Meeting The Inst. Navigat.*, Feb. 2021, pp. 282–294.

[228] J. Arribas, M. A. Gómez, C. Fernández-Prades, D. L. Martín, J. M. García-Tuñón, and T. G. Rioja, "A receiver-independent GNSS smart antenna for simultaneous jamming and spoofing protection," in *Proc. IEEE Aerosp. Conf.*, Mar. 2023, pp. 1–13.

[229] A. Venturino, E. D'Afflisio, N. Forti, P. Braca, P. Willett, and M. Z. Win, "Adaptive resilience navigation filter for detecting and mitigating multispoofing attacks in range-based localization systems using antenna arrays," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 61, no. 3, pp. 6856–6872, Jun. 2025.
[230] 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 J.*, vol. 22, no. 23, pp. 23423–23435, Dec. 2022.
[231] D. K. Panda and W. Guo, "Action robust reinforcement learning for air mobility deconfliction against conflict induced spoofing," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 12, pp. 21343–21355, Dec. 2024.
[232] J. Tang et al., "Improving GNSS positioning correction using deep reinforcement learning with an adaptive reward augmentation method," *NAVIGATION, J. Inst. Navigat.*, vol. 71, no. 4, 2024, Art. no. navi.667.
[233] J. Hu, M. Ammar, B. Z. Hussain, J. Kim, and I. Khan, "Reinforcement-learning-driven integrated detection and mitigation of UAV GPS spoofing attacks," *IEEE Internet Things J.*, vol. 12, no. 18, pp. 36926–36941, Sep. 2025.
[234] A. Eldosouky, A. Ferdowsi, and W. Saad, "Drones in distress: A game-theoretic countermeasure for protecting UAVs against GPS spoofing," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2840–2854, Apr. 2020.
[235] C. Huang et al., "To lock the authentic signals: Mitigating GNSS spoofing with INS-aided tracking," *Inf. Fusion*, vol. 126, Feb. 2026, Art. no. 103596.
[236] Y. Hao, C. Shi, A. Xu, X. Sui, and M. Xia, "Revealing methods of GNSS spoofing mitigation through analyzing the spoofing impacts on adaptively robust estimation-based RTK/INS tightly coupled integration," *IEEE Sensors J.*, vol. 23, no. 20, pp. 25165–25178, Oct. 2023.
[237] X. Shang, F. Sun, B. Liu, L. Zhang, and J. Cui, "GNSS spoofing mitigation with a multicorrelator estimator in the tightly coupled INS/GNSS integration," *IEEE Trans. Instrum. Meas.*, vol. 72, pp. 1–12, 2023.
[238] J. Chang, Y. Zhang, S. Fan, F. Huang, D. Xu, and L.-T. Hsu, "An anti-spoofing model based on MVM and MCCM for a loosely-coupled GNSS/INS/LiDAR Kalman filter," *IEEE Trans. Intell. Vehicles*, vol. 9, no. 1, pp. 1744–1755, Jan. 2024.
[239] Q. Yang, Y. Zhang, B. Lian, and C. Tang, "Airborne GPS interference cancellation algorithm based on deep learning," in *Proc. I_{ON} GNSS+, Int. Tech. Meeting Satell. Division Inst. Navigat.*, Nov. 2017, pp. 1695–1700.
[240] J. Song, Z. Lu, X. Zhao, W. Xiao, X. Tang, and G. Sun, "GNSS multiple interference mitigation with TF-UNet method based on high-resolution interference sensing," *IEEE Sensors J.*, vol. 26, no. 1, pp. 1358–1369, Jan. 2026.
[241] M. Wentz, J. Capper, B. Kurien, K. Forsythe, and K. Chowdhury, "Blind beamforming via deep learning-based signal classification and transfer learning," *IEEE Trans. Cognit. Commun. Netw.*, vol. 12, pp. 1834–1847, 2026.
[242] N. T. T. Uyen, D. D. Hung, L. T. Binh, P. T. Hiep, and N. T. Phuong, "Deep learning-based beamforming for multi-user active electronically scanned array systems," *Signal, Image Video Process.*, vol. 19, no. 14, p. 1229, Dec. 2025.
[243] F. Chen, L. Huang, Q. Zhou, and C. Ren, "GNSS cognitive interference mitigation method based on deep learning," in *Proc. 5th Int. Conf. Electron. Commun. Artif. Intell. (ICECAI)*, May 2024, pp. 8–14.
[244] M. Appel, A. Konovaltsev, and M. Meurer, "Robust spoofing detection and mitigation based on direction of arrival estimation," in *Proc. 28th Int. Tech. Meeting The Satell. Division Inst. Navigat. (ION GNSS+)*, 2015, pp. 3335–3344.
[245] X. Shang et al., "GNSS spoofing detection based on multicorrelator distortion monitoring," *GPS Solutions*, vol. 27, no. 2, p. 94, Apr. 2023.
[246] B. Ren, F. Chen, S. Ni, C. Han, Z. Lu, and S. Han, "Performance analysis of repeater spoofing suppression based on GNSS multi-beam receiver," *Frontiers Phys.*, vol. 10, Aug. 2022, Art. no. 970132.
[247] Y. Zhao, F. Shen, G. Xu, and G. Wang, "A spatial–temporal approach based on antenna array for GNSS anti-spoofing," *Sensors*, vol. 21, no. 3, p. 929, Jan. 2021.
[248] S. Wang, J. Liu, B.-G. Cai, J. Wang, and D.-B. Lu, "GNSS spoofing detection and elimination for resilient train positioning using spiking neural network and compressed sensing," in *Proc. IEEE 27th Int. Conf. Intell. Transp. Syst. (ITSC)*, Sep. 2024, pp. 2172–2178.
[249] L. Li, X. Jing, H. Liu, H. Lei, and Q. Chen, "Adaptive anti-jamming resource allocation scheme in dynamic jamming environment," *IEEE Trans. Veh. Technol.*, vol. 74, no. 7, pp. 1–11, Jul. 2025.
[250] E. A. Marranghelli, R. L. La Valle, and P. A. Roncagliolo, "Simple and effective GNSS spatial processing using a low-cost compact antenna array," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 57, no. 5, pp. 3479–3491, Oct. 2021.
[251] X. Hu, L. Chu, J. Pei, W. Liu, and J. Bian, "Model complexity of deep learning: A survey," *Knowl. Inf. Syst.*, vol. 63, no. 10, pp. 2585–2619, Oct. 2021.
[252] Z. Yin, Y. Lin, Y. Zhang, Y. Qian, F. Shu, and J. Li, "Collaborative multiagent reinforcement learning aided resource allocation for UAV anti-jamming communication," *IEEE Internet Things J.*, vol. 9, no. 23, pp. 23995–24008, Dec. 2022.
[253] Z. Zuo, B. Yang, Z. Li, and T. Zhang, "A GNSS/IMU/vision ultra-tightly integrated navigation system for low altitude aircraft," *IEEE Sensors J.*, vol. 22, no. 12, pp. 11857–11864, Jun. 2022.
[254] J. Zhou, W. Wang, X. Hong, and C. Zhang, "Multi-UAV cooperative anti-jamming for GNSS signals based on frequency-domain power inversion," *IEEE Sensors J.*, vol. 24, no. 19, pp. 30778–30791, Oct. 2024.
[255] J. Zhou, W. Wang, and C. Zhang, "A GNSS anti-jamming method in multi-UAV cooperative system," *IEEE Trans. Veh. Technol.*, vol. 75, no. 1, pp. 535–547, Jan. 2026.
[256] G. Marut, T. Hadas, and J. Nosek, "Intercomparison of multi-GNSS signals characteristics acquired by a low-cost receiver connected to various low-cost antennas," *GPS Solutions*, vol. 28, no. 2, p. 82, Apr. 2024.
[257] S. Ni et al., "GNSS spoofing suppression based on multi-satellite and multi-channel array processing," *Frontiers Phys.*, vol. 10, Jun. 2022, Art. no. 905918.
[258] H. Ge et al., "LEO enhanced global navigation satellite system (LeGNSS): Progress, opportunities, and challenges," *Geo-Spatial Inf. Sci.*, vol. 25, no. 1, pp. 1–13, Jan. 2022.
[259] W. Stock, R. T. Schwarz, C. A. Hofmann, and A. Knopp, "Survey on opportunistic PNT with signals from LEO communication satellites," *IEEE Commun. Surveys Tuts.*, vol. 27, no. 1, pp. 77–107, Feb. 2025.
[260] W. Zheng, S. Lu, Y. Yang, Z. Yin, and L. Yin, "Lightweight transformer image feature extraction network," *PeerJ Comput. Sci.*, vol. 10, p. e1755, Jan. 2024.
[261] J. Pfeiffer, S. Ruder, I. Vulić, and E. M. Ponti, "Modular deep learning," 2023, *arXiv:2302.11529*.
[262] J. Gou, B. Yu, S. J. Maybank, and D. Tao, "Knowledge distillation: A survey," *Int. J. Comput. Vis.*, vol. 129, no. 6, pp. 1789–1819, 2021.
[263] Y. Zhuang et al., "Multi-sensor integrated navigation/positioning systems using data fusion: From analytics-based to learning-based approaches," *Inf. Fusion*, vol. 95, pp. 62–90, Jul. 2023.
[264] L. Xiang, F. Wang, W. Xu, T. Zhang, M. Pan, and Z. Han, "Dynamic UAV swarm collaboration for multi-targets tracking under malicious jamming: Joint power, path and target association optimization," *IEEE Trans. Veh. Technol.*, vol. 73, no. 4, pp. 5410–5425, Apr. 2024.
[265] M. Liu, Z. Liu, W. Lu, Y. Chen, X. Gao, and N. Zhao, "Distributed few-shot learning for intelligent recognition of communication jamming," *IEEE J. Sel. Topics Signal Process.*, vol. 16, no. 3, pp. 395–405, Apr. 2022.
[266] A. Siemuri, K. Selvan, H. Kuusniemi, P. Valisuo, and M. S. Elmusrati, "A systematic review of machine learning techniques for GNSS use cases," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 6, pp. 5043–5077, Dec. 2022.
[267] L. Jia et al., "Game theory and reinforcement learning for anti-jamming defense in wireless communications: Current research, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 27, no. 3, pp. 1798–1838, Jun. 2025.
[268] S. B. Janiar and P. Wang, "Intelligent anti-jamming based on deep reinforcement learning and transfer learning," *IEEE Trans. Veh. Technol.*, vol. 73, no. 6, pp. 8825–8834, Jun. 2024.



Yejia Zeng received the B.S. degree in communication engineering from the University of Electronic Science and Technology of China, Chengdu, China, in 2023. He is currently pursuing the Ph.D. degree with the College of Electronic Science and Technology, National University of Defense Technology, Changsha, China. His research interests include signal processing, anti-interference technologies for satellite navigation systems, wireless communication, and robust navigation for uncrewed aerial vehicles (UAVs), with a focus on enhancing the security and reliability of navigation in challenging environments.

Zukun Lu received the B.S. and M.S. degrees from Chinese Aviation University of Air Force, Changchun, in 2011 and 2013, respectively, and the Ph.D. degree from the College of Electronic Science and Technology, National University of Defense Technology, Changsha, China. Since 2014, he has been with the College of Electronic Science and Technology, National University of Defense Technology, where he is currently a Senior Engineer. His current research interests include satellite-based navigation anti-jamming and measurements.

Xiaoyu Zhao received the B.S. degree in communication engineering from Hunan Institute of Technology, Hengyang, China, in 2016, the M.S. degree in information and communication engineering from Guilin University of Electronic Technology, Guilin, China, in 2019, and the Ph.D. degree in information and communication engineering from Xidian University, Xi'an, China, in 2024. He is currently with the National University of Defense Technology. His research interests include distributed cooperative localization and satellite-based navigation anti-jamming and measurement.

Zhu Xiao (Senior Member, IEEE) received the M.S. and Ph.D. degrees in communication and information systems from Xidian University, Xi'an, China, in 2007 and 2009, respectively. From 2010 to 2012, he was a Research Fellow with the Department of Computer Science and Technology, University of Bedfordshire, Luton, U.K. He is currently a Full Professor with the College of Computer Science and Electronic Engineering, Hunan University, Changsha, China. His research interests include intelligent information processing, the Internet of Vehicles, and wireless communications systems. He is serving as an Associate Editor for IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS.

Shaojie Ni received the M.S. and Ph.D. degrees in electrical engineering from the National University of Defense Technology, Changsha, China. He is currently with the College of Electronic Science and Technology, National University of Defense Technology. He has long been involved in the construction and application promotion of the Beidou Navigation Satellite System and has served as a principal investigator for numerous projects. His research interests include navigation and spatiotemporal positioning, satellite payload, navigation terminal technology, and the national integrated positioning, navigation, and timing (PNT) systems.

Zhu Han (Fellow, IEEE) received the B.S. degree in electronic engineering from Tsinghua University in 1997 and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, MD, USA, in 1999 and 2003, respectively. From 2000 to 2002, he was a Research and Development Engineer with JDSU, Germantown, MD, USA. From 2003 to 2006, he was a Research Associate with the University of Maryland. From 2006 to 2008, he was an Assistant Professor with Boise State University, Boise, ID, USA. Currently, he is a John and Rebecca Moores Professor with the Electrical and Computer Engineering Department and the Computer Science Department, University of Houston, Houston, TX, USA. He is also an honored Lifetime Chair Professor with National Yang Ming Chiao Tung University, Taiwan, an Eminent Scholar with Kyung Hee University, South Korea, and a Global Professor with Keio University, Japan. His main research targets the novel game-theory-related concepts critical to enabling efficient and distributive use of wireless networks with limited resources. His other research interests include wireless resource allocation and management, wireless communications and networking, quantum computing, data science, smart grids, carbon neutralization, and security and privacy. He has been an AAAS Fellow since 2019 and an ACM Fellow since 2024. He received the NSF Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for the Journal on Advances in Signal Processing in 2015, the IEEE Leonard G. Abraham Prize in the field of Communications Systems (Best Paper Award in IEEE JSAC) in 2016, the IEEE Vehicular Technology Society 2022 Best Land Transportation Paper Award, and several best paper awards in IEEE conferences. He was an IEEE Communications Society Distinguished Lecturer from 2015 to 2018 and an ACM Distinguished Speaker from 2022 to 2025. He is also the Winner of the 2021 IEEE Kiyo Tomiyasu Award (an IEEE Field Award), for outstanding early to mid-career contributions to technologies holding the promise of innovative applications, with the following citation: "for contributions to game theory and distributed management of autonomous communication networks."

Keqin Li (Fellow, IEEE) received the B.S. degree in computer science from Tsinghua University, China, in 1985, and the Ph.D. degree in computer science from the University of Houston in 1990. He is currently a SUNY Distinguished Professor with the State University of New York at New Paltz. He is also a National Distinguished Professor at Hunan University, China. He has authored or co-authored more than 1270 journal articles, book chapters, and refereed conference papers. He holds nearly 80 patents announced or authorized by Chinese National Intellectual Property Administration. He is a member of Academia Europaea (MAE), European Academy of Sciences and Arts (EASA), USA National Academy of Artificial Intelligence (NAAI), the World Academy of Sciences (WAS), and the SUNY Distinguished Academy, a fellow of American Association for the Advancement of Science (AAAS), the International Academy of Artificial Intelligence Sciences (AAIS), the International Artificial Intelligence Industry Alliance (AIIA), the World Academy of Engineering and Technology (WAET), and Asia Computational Intelligence Society (ACIS). He is among the world's top few most influential scientists in parallel and distributed computing, regarding single-year impact (ranked #2) and career-long impact (ranked #3) based on a composite indicator of the Scopus citation database. He is listed in Scilit Top Cited Scholars and is among the top 0.02% out of more than 20 million scholars worldwide based on top-cited publications in the last ten years. He is listed in ScholarGPS Highly Ranked Scholars and is among the top 0.002% out of more than 30 million scholars worldwide based on a composite score of three ranking metrics for research productivity, impact, and quality in the recent five years.