frontiers | Frontiers in Physics

TYPE Review
PUBLISHED 17 December 2024
DOI 10.3389/fphy.2024.1428544

OPEN ACCESS

EDITED BY
Zhu Xiao,
Hunan University, China

REVIEWED BY
Mandeep Singh,
National Institute of Technology, India
Jan M. Kelner,
Military University of Technology (WAT), Poland

*CORRESPONDENCE
Zukun Lu,
luzukun@nudt.edu.cn

RECEIVED 06 May 2024
ACCEPTED 23 September 2024
PUBLISHED 17 December 2024

CITATION
Lu C, Lu Z, Liu Z, Huang L and Chen F (2024) Overview of satellite nav spoofing and anti-spoofing techniques.
Front. Phys. 12:1428544.
doi: 10.3389/fphy.2024.1428544

Overview of satellite nav spoofing and anti-spoofing techniques

Cheng Lu[1], Zukun Lu[1,2]*, Zhe Liu[1,2], Long Huang[1,2] and Feiqiang Chen[1,2]

[1]College of Electronic and Technology, National University of Defense Technology, Changsha, China, [2]Key Laboratory of Satellite Navigation Technology, Changsha, China

In recent years, satellite navigation systems have witnessed widespread adoption across diverse fields, including military surveillance, precision agriculture, traffic monitoring, resource exploration, and disaster assessment. However, navigation signals are susceptible to interference, with deceptive interference posing the most significant threat to navigation systems. This paper provides a comprehensive overview of satellite navigation spoofing and anti-spoofing techniques. It reviews the current state of spoofing and anti-spoofing technologies, analyzing advancements in spoofing techniques and the evolution of countermeasures. Furthermore, the paper elaborates on the impact of spoofing interference on receiver performance, examining its effects on positioning, timing, and velocity estimations. A detailed analysis of various anti-spoofing methods is presented, categorizing them into detection, identification, suppression, and localization techniques. This review aims to provide a thorough understanding of the evolving landscape of satellite navigation spoofing and anti-spoofing technologies, fostering further research and development efforts to ensure the integrity and resilience of satellite navigation systems in the face of sophisticated threats.

KEYWORDS

satellite navigation, generative spoofing jamming, induced deceptive jamming, induced deceptive jamming monitoring, induced spoofing interference suppression

1 Introduction

Global navigation satellite systems (GNSSs) provide ground users with continuous, all-weather, high-precision positioning, timing, and velocity information through navigation signals transmitted from artificial satellites [1]. The remarkable performance of GNSSs has led to their widespread adoption across civilian and military domains [2].

As shown in Figure 1, in the military domain, modern warfare increasingly relies on high-precision positioning and velocity data for the precise control of precision-guided weapons, aircraft, ships, and various vehicular equipment. Satellite navigation systems are thus a critical enabler for land, sea, and air weapon systems, facilitating the construction of fully digitized battlefields.

GNSS technology has permeated many industries in the civilian domain, including providing precise timing for power systems, navigation for civil aviation and vehicles, and high-precision positioning and timing services for ship navigation. It plays a crucial role in disaster relief efforts and numerous aspects of daily life, becoming an indispensable component of modern society's infrastructure.

Navigation signals, typically transmitted from satellites to ground receivers, are susceptible to various intentional and unintentional disruptions due to long-distance propagation and low signal power at ground reception [3, 4]. Moreover, the

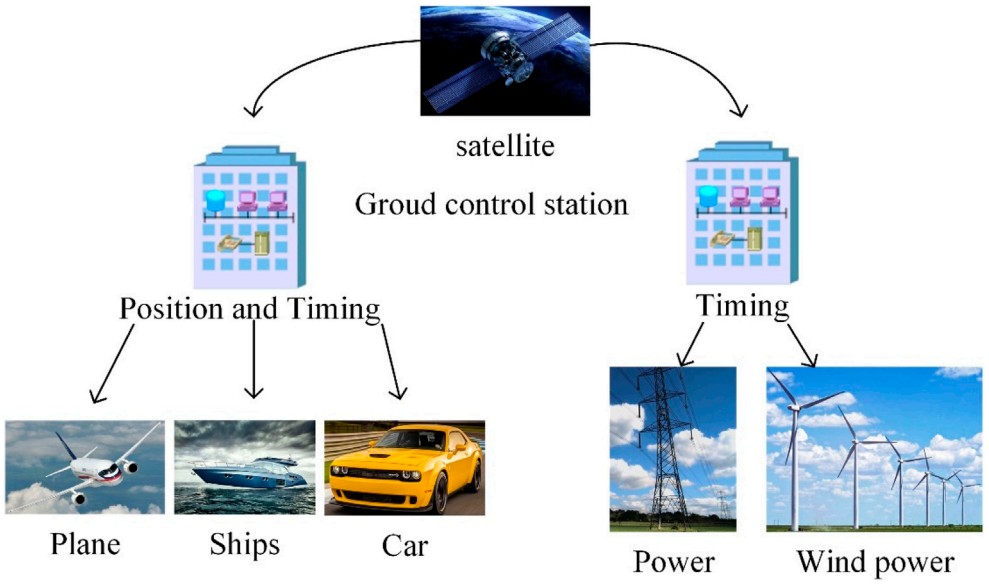

FIGURE 1
Role of satellites in civil navigation.

information transparency and open signal characteristics of navigation systems [5, 6], particularly the detailed specifications and descriptions of civilian GNSS control interface documents (ICDs) regarding carrier frequency, modulation schemes, and navigation messages [7], make them highly vulnerable to information tampering and deceptive spoofing attacks, posing significant threats to navigation systems. Spoofing signals, with power levels comparable to genuine navigation signals, exhibit high stealthiness and efficiently disrupt navigation receivers, resulting in inaccurate positioning and timing information and potentially catastrophic consequences [8]. This is particularly concerning in the case of drones, where spoofing interference can manipulate the drone's navigation system through pseudo-range spoofing, leading to erroneous positioning results [9, 10].

This paper delves into the mechanisms of GNSS spoofing attacks and explores a range of countermeasures. The paper begins by examining the vulnerabilities of GNSS receivers to spoofing attacks, highlighting the security threats they pose. It then analyzes the strategies and mechanisms employed in spoofing attacks, providing a comprehensive overview of different attack methodologies. The paper further examines the impact of spoofing signals on targeted receivers, delving into the underlying principles of induced spoofing attacks and their rapid evolution in recent years. Subsequently, the paper explores various anti-spoofing technologies tailored to counter different spoofing attacks. This includes an analysis of five signal-level spoofing detection techniques, examining advancements in deep learning-based spoofing identification techniques and providing a summary of the application scenarios and performance characteristics of various anti-spoofing technologies. Finally, the paper concludes by presenting methods for locating the source of spoofing interference.

To make it easier for readers to understand this survey, Table 1 lists some important abbreviations and their meanings. These abbreviations apply only to this survey. Specific explanations are given in Table 1.

2 Current status and case studies of spoofing

The concept of spoofing interference in satellite navigation systems, first detailed in 2003 by British researchers D.J. Shepherd and M.G. Bitterlin [11], has transitioned from a theoretical possibility to a demonstrable reality [12]. Early research outlined the potential for such attacks and proposed basic countermeasures, but advancements in technology and increasing threats have spurred further investigation and a deeper understanding of spoofing interference. The danger has manifested in real-world scenarios, with notable examples including the capture of American unmanned reconnaissance aircraft, "RQ-170" and "Scan Eagle," by Iranian forces in 2011 and 2012, respectively [13, 14]. These operations reportedly employed spoofing techniques to disrupt communication between the drones and their satellites, transmitting deceptive signals that lured them to land. Further experiments conducted by Professor Todd Humphreys' team in 2012 demonstrated the feasibility of hijacking GPS-guided drones and manipulating their navigation systems using spoofing signals [15]. Later that year, the team successfully hijacked a civilian drone at the U.S. Army's White Sands Missile Range, highlighting the vulnerability of civilian drones to spoofing attacks [16]. In 2013, the team demonstrated the potential for spoofing attacks at sea by successfully diverting an $80 million yacht from its course using a compact GPS spoofing jammer [16]. These experiments, along with others conducted by M.L. Psiakiand and T.E. Humphreys in 2017 [17], underscore the susceptibility of GNSS receivers to spoofing attacks and the challenge for users in detecting such interference.

In April 2013, at the Hack in the Box security conference in Amsterdam, Hugo Teso, a commercial pilot and engineer from a German cybersecurity company, unveiled the PlaneSploit application, a tool capable of bypassing aircraft security systems

TABLE 1 Abbreviations table.

Abbreviation	Meaning	Abbreviation	Meaning
AOA	Angle of arrival	BPNN	Backpropagation neural network
CDMA	Code division multiple access	CNN	Convolutional neural network
CNR	Carrier-to-noise ratio	CRPD	Carrier-phase single difference
CSI	Channel state information	DLLS	Delay-locked loops
FDOA	Frequency difference of arrival	FLLS	Frequency-locked loops
FWHM	Full width half maxima	GNSS	Global navigation satellite system
GSI	Generative spoofing interference	ICD	Interface control document
IF	Intermediate frequency	INS	Inertial navigation units
MIMO	Multiple-input multiple-output	PLLS	Phase-locked loops
PRN	Pseudo-random noise code	PRDD	Pseudo-range double differences
RAIM	Receiver autonomous integrity monitoring	RF	Radio frequency
SNR	Signal-to-noise ratio	SQM	Signal quality monitoring
SVM	Support vector machines	TDOA	Time difference of arrival
TOA	Time of arrival	UAV	Unmanned aerial vehicle

and gaining control of the aircraft's computer systems [18]. Teso successfully demonstrated PlaneSploit's capabilities by altering the flight path, adjusting air conditioning settings, and even simulating a crash landing, highlighting the significant risks posed by such attacks. In 2017, the Unicorn Team, a hacking group affiliated with 360 company, further demonstrated the feasibility of spoofing civilian GPS devices at the Def Con hacking conference in the United States. Later that year, they showcased their ability to spoof the BeiDou navigation system at the POC hacking conference, demonstrating the global reach of spoofing capabilities. In 2018, the U.S. Navy conducted a real-world spoofing attack simulation exercise named "Sea Lion Father" in the Pacific Ocean. The exercise involved using false GPS signals to disrupt the electronic equipment of their vessels, effectively counteracting the real positioning capabilities of their location and navigation systems. This exercise highlighted the potential for spoofing to disrupt critical maritime operations, emphasizing the urgent need for robust countermeasures.

3 Analysis of spoofing interferes

Satellite navigation signals employ direct sequence spread spectrum modulation composed of three components: carrier, pseudo-random code, and navigation message data code. The carrier, residing at the bottom layer of the satellite navigation signal, carries the pseudocode and navigation message. The pseudo-random code is used primarily for spreading the data code, and the data code stores the satellite ephemeris. The specific signal can be represented by the following Equation 1:

$$S(t) = \mathrm{A} \times C(t) \times D(t) \times \cos(\omega t + \varphi). \quad (1)$$

A represents the amplitude, $C(t)$ represents pseudocode, $D(t)$ represents the data code, ω represents the carrier frequency, and φ represents the carrier phase.

Spoofing operates by transmitting signals that mimic the format of authentic satellite navigation signals with altered parameters, targeting the receiver. The receiver, unaware of the manipulation, captures and tracks these spoofed signals, resulting in erroneous positioning and timing data. There are two primary categories of spoofing interference: generative spoofing and forwarding spoofing.

3.1 Relay-based spoofing interference

Relay-based spoofing interference operates by forwarding intercepted genuine satellite navigation signals, effectively extending their propagation time and introducing inaccuracies into positioning results [19, 20]. To ensure that the relayed spoofed signal is captured and tracked by the receiver, it is typically transmitted with a power approximately 2 dB higher than the genuine satellite signal [21]. Relay-based spoofing interference can be categorized into two types: single-antenna and multi-antenna. Single-antenna relay-based spoofing utilizes a single omnidirectional antenna to receive, amplify, delay, and forward signals from all satellites within its field of view. As the interference device introduces the same additional delay to all visible satellite signals, this method can induce deviations in the target receiver's positioning but cannot precisely control or set the final position. Multi-antenna relay-based spoofing interference, however, employs multiple omnidirectional antennas, each corresponding to a visible satellite in its field of view. This allows for the introduction of distinct delays and Doppler shifts to each visible satellite signal, enabling precise control over the target receiver's positioning and even directing it to a predetermined false location. In terms of effectiveness and covertness, multi-antenna relay-based spoofing interference aligns better with the requirements of future information warfare, such as navigation warfare and time warfare. Its potential applications in these domains make it a valuable area of ongoing research.

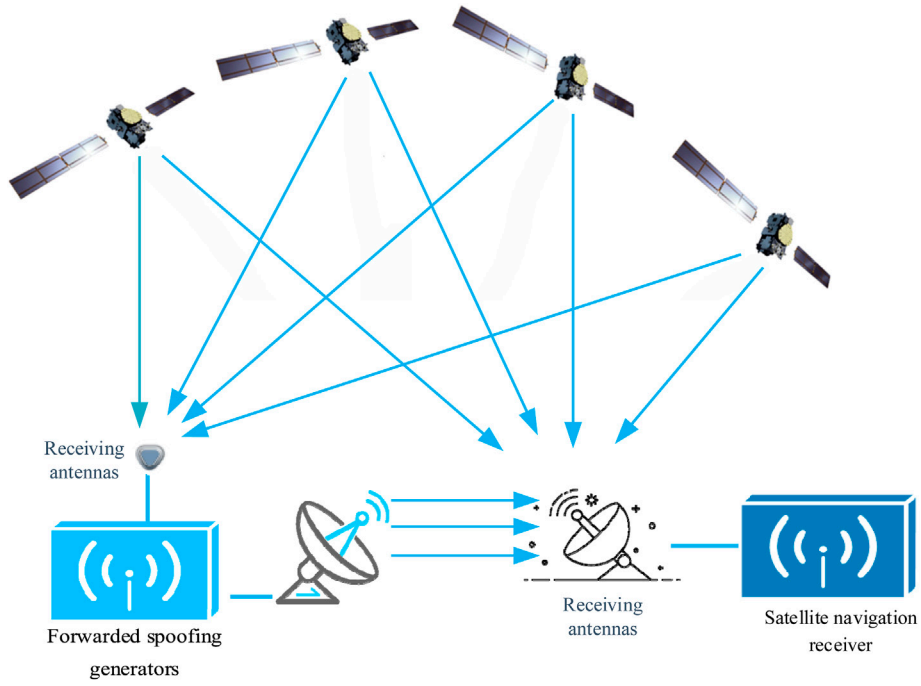

FIGURE 2
Schematic diagram of relay-based spoofing interference.

Despite its advantages, current research has identified a significant drawback of multi-antenna relay-based spoofing interference. When the distance between the interference device and the target receiver exceeds a certain range, it can cause abrupt jumps in the clock bias calculated by the target receiver. The receiver can successfully identify this type of spoofing by performing integrity monitoring and analysis on the calculated clock bias data. This limitation significantly restricts the operational range of multi-antenna relay-based spoofing interference. The primary solution proposed for this issue involves demodulating the satellite signal and manipulating the code phase of the pseudo-random noise code (PRN) sequence to compensate for the additional clock bias introduced at the target receiver. However, demodulating the satellite signal requires knowledge of the signal structure and PRN sequence, making it unsuitable for military signals [22]. Figure 2 illustrates the architecture of a relay-based spoofing interference system. Distributed relay-based spoofing interference leverages natural or controllable propagation delays during signal forwarding to disrupt receiver operations. Due to the confidential nature of the M-code, relay-based spoofing has become a key focus for targeting military codes.

Simultaneously, regional augmentation techniques based on pseudo-satellites have matured [23]. Building upon this foundation, literature [24] proposes a regional navigation and spoofing interference integrated system based on pseudo-satellites. This system consists of three components: a relay-based interferer, a carrier platform, and a ground control station. The relay-based interferer, positioned approximately 20 km above ground, generates interference signals. The ground control station controls the carrier platform's location and transmits instructions to the interferer, controlling the magnitude of the introduced delay in the forwarded signal. This system utilizes controlled forwarding delays to achieve regional mapping spoofing interference. Concurrently, code division multiple access (CDMA) technology is employed to superimpose the platform's location information and the introduced delay information onto the forwarded signal. As the friendly spread spectrum signal is orthogonal to the forwarded signal, the two signals act as noise to each other without mutual interference. Enemy GPS receivers acquire erroneous delay information, mapping the true location (R) to a virtual location (F), achieving spoofing interference. Simultaneously, friendly receivers obtain the carrier platform's location information and compensate for the delay, allowing for their navigation and positioning. The system principle is illustrated in Figure 3.

3.2 Generative spoofing interference

Generative spoofing interference is created by a satellite signal simulator that autonomously generates signals that mimic real satellite navigation signals based on known signal characteristics, including carrier frequency, C/A code, code phase, and modulation scheme [25]. These spoofed signals are synchronized with genuine signals to create a deceptive effect. Figure 4 illustrates the architecture of a generative spoofing interference system.

Generative spoofing interference (GSI) can be categorized into three levels based on its implementation complexity: primary, intermediate, and advanced [26–28]. Primary GSI relies on satellite signal simulators to generate spoofing signals without synchronizing parameters with the genuine signal, resulting in weak spoofing capabilities. Intermediate GSI, on the other hand, estimates the genuine satellite signal parameters, such as power,

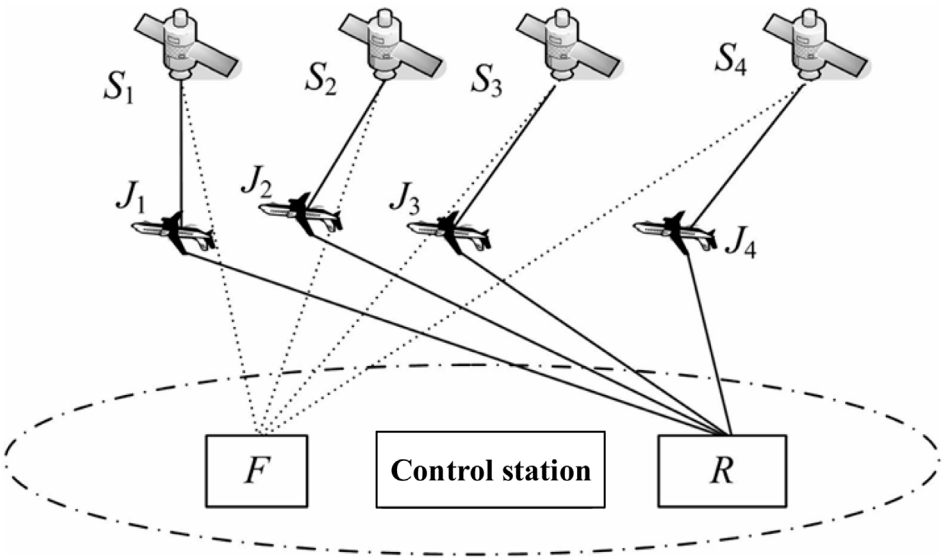

FIGURE 3
Schematic diagram of a GPS decoy jamming and regional navigation-integrated system [24].

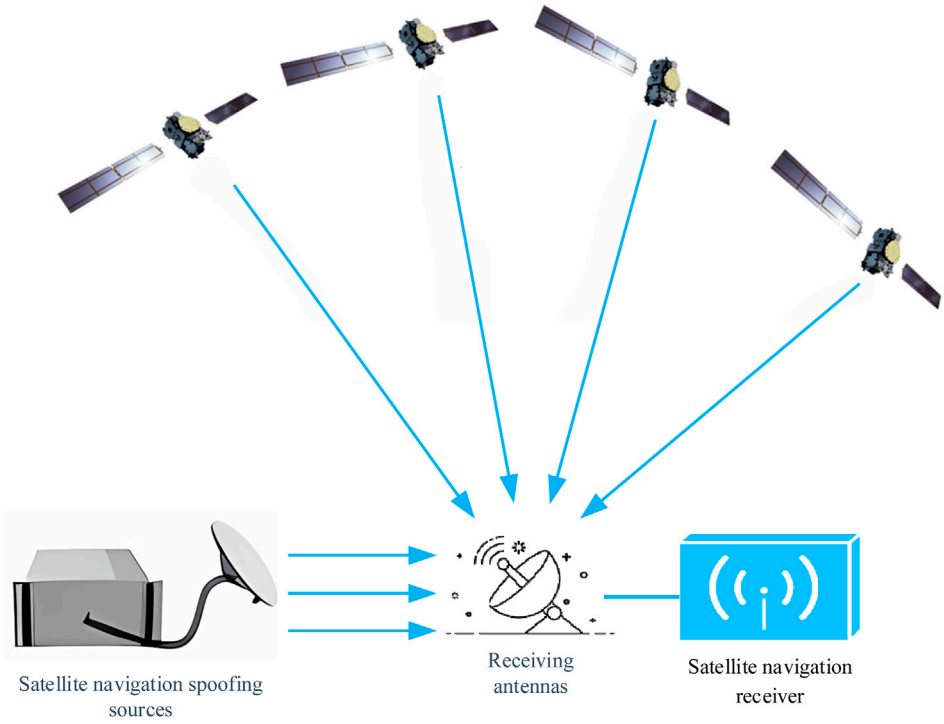

FIGURE 4
Schematic diagram of generative spoofing interference.

code phase, carrier frequency, navigation message, and modulation scheme. This enables the spoofing signal to mimic the genuine signal in terms of signal structure, thus increasing the likelihood of deceiving target receivers [29]. Advanced GSI builds upon intermediate GSI by employing multiple intermediate GSI sources for joint spoofing, overcoming the limitations of single-antenna transmission. It further integrates beamforming techniques to perfectly synchronize spoofing signals in parameters such as arrival angle. Intermediate GSI is the most widely adopted and successful technique, with the highest intrusion success rate. This paper focuses on intermediate GSI. The core principle of intermediate GSI lies in parameter synchronization with the

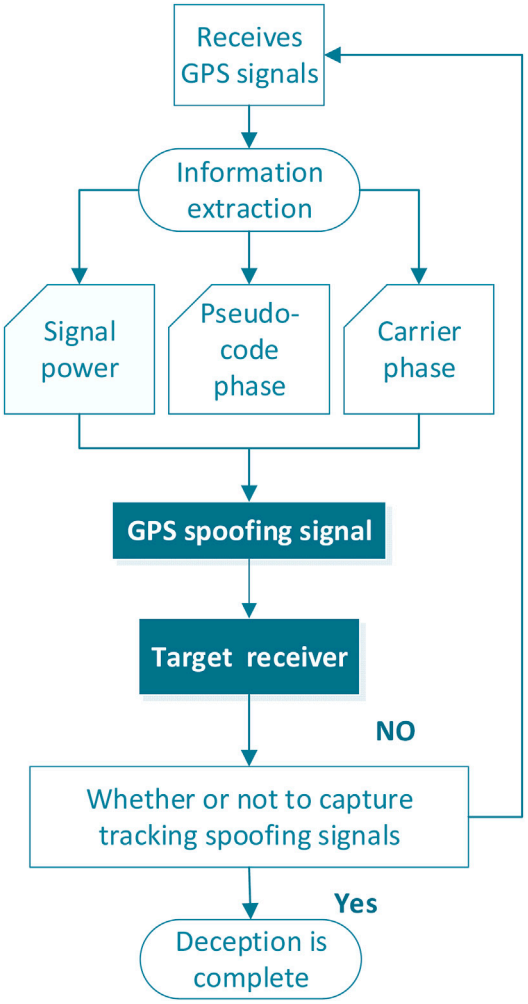

FIGURE 5
Intermediate generative deception interference flowchart.

genuine signal, including power, carrier frequency, code phase, modulation scheme, and navigation message synchronization. This ensures the spoofing signal can successfully decouple the genuine signal within the tracking loop of the satellite navigation receiver, thus facilitating the receiver to track the spoofing signal and achieve the spoofing effect. Figure 5 illustrates the general workflow of intermediate GSI.

As illustrated in Figure 5, the implementation process of intermediate generative spoofing interference can be described as follows: Initially, the satellite signal receiver in the spoofing interference module captures, tracks, and decodes the authentic signal, obtaining the code phase, carrier phase, received power, and navigation message of the authentic signal. Subsequently, the obtained parameters are utilized to adjust the parameters of the spoofed signal. Finally, the spoofed signal is modulated and transmitted.

The spoofed signal arrives at the receiver alongside the authentic signal. Generally, the power of the spoofed signal exceeds the power of the authentic signal by 3 dB. Under the power advantage of the spoofed signal, the receiver will abandon tracking the authentic signal and switch to tracking the spoofed signal, effectively completing the spoofing of the satellite navigation receiver. For receivers already tracking the genuine signal, capturing other search units will not affect the channel. Therefore, a corresponding phase induction model is required to execute spoofing interference against a receiver already in tracking mode while maintaining the lock. This model employs phase induction to perform covert spoofing against the receiver. This can be further categorized into synchronous induction and asynchronous induction [30] based on the different induction methods.

3.2.1 Induced spoofing interference analysis

The GPS radio frequency (RF) signal received by the antenna cannot be directly processed at the user receiver. It first needs to undergo down conversion by the RF front-end, followed by necessary filtering and gain control to obtain the GPS intermediate frequency (IF) signal. Finally, the IF signal is fed into the receiver for signal processing and position calculation.

The signal structure of an induced spoofing signal is identical to that of a genuine satellite signal. Therefore, the IF signal entering the receiver can be represented by Equations 2, 3, respectively [31]:

$$x_a(t) = \sum_{i=1}^{N_a} \sqrt{P_a^i(t)} D^i(t-\tau_a^i) C^i(t-\tau_a^i) \cos\left(2\pi\left(f_0 + f_{d,a}^i\right)t + \phi_a^i\right), \tag{2}$$

$$x_s(t) = \sum_{i=1}^{N_s} \sqrt{P_s^i(t)} D^i(t-\tau_s^i) C^i(t-\tau_s^i) \cos\left(2\pi\left(f_0 + f_{d,s}^i\right)t + \phi_s^i\right). \tag{3}$$

In this formula, $x_a(t)$ and $x_s(t)$ represent the real satellite signal and the spoofing signal, N_a and N_s represent the number of satellites included, P_a^i and P_s^i represent the signal power, $D^i(t)$ represents the navigation data message, $C^i(t)$ represents the C/A code, τ_a^i and τ_s^i represent the code phase of each signal, f_0 represents the intermediate frequency (IF), $f_{d,a}^i$ and $f_{d,s}^i$ represent the Doppler shift of the signals, and ϕ_a^i and ϕ_s^i represent the initial phase of the carrier of the signals, respectively. Therefore, when induced spoofing interference is present, the receiver mixed IF signal would have both a real satellite signal and a spoofing signal:

$$x(t) = x_a(t) + x_s(t) + n(t), \tag{4}$$

where $n(t)$ represents Gaussian white noise with a mean value of 0.

The satellite signal must be captured before the receiver performs the signal processing part. This process is a rough estimate of the carrier frequency and code phase of the satellite signal. The principle is to use the local end of the receiver to generate a signal with a certain carrier frequency and code phase and then correlate and mix the received signal with the local replication signal to detect the correlation degree between the two. When the correlation between the received signal and the local signal exceeds the preset capture threshold, the carrier phase and code phase of the local replicated signal can be roughly assumed to be the same as that of the real satellite signal. However, the signal acquisition is only a rough estimation of the parameters of the received satellite signal, which is not enough to meet the requirements of positioning and solving. Accurate estimation of the satellite signal parameters also needs the receiver to enter the tracking loop to be realized. Induced spoofing jamming is a kind of covert spoofing jamming, which usually implements spoofing after

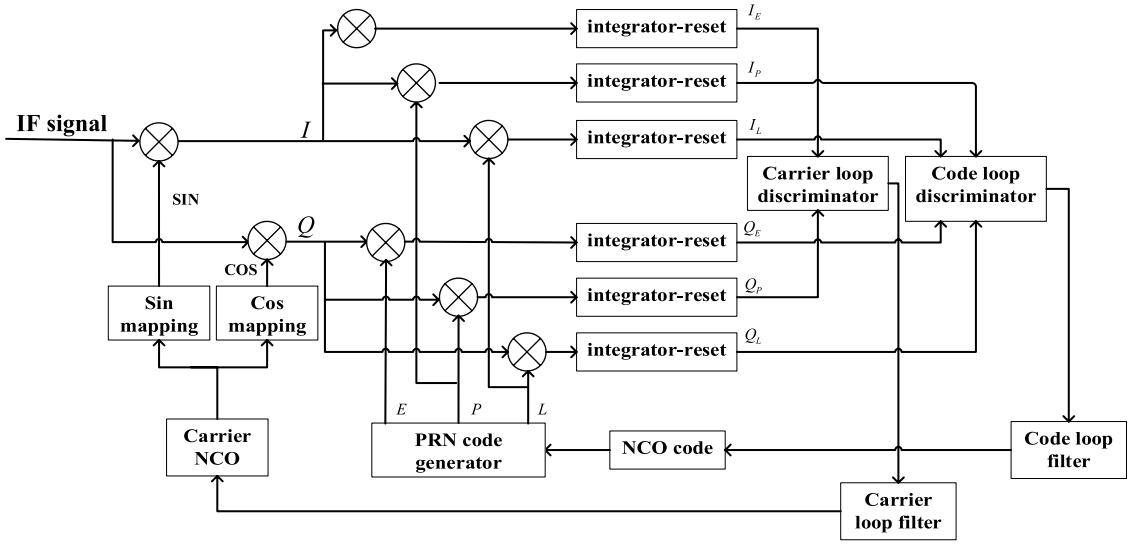

FIGURE 6
General schematic diagram of the receiver tracking loop.

the receiver enters the tracking stage and cannot interrupt the tracking state of the receiver's tracking loop, so the impact of induced spoofing jamming on the receiver is mainly reflected in the tracking loop. Due to the continuous relative motion between the receiver and the satellite, the pseudocode phase, carrier phase, and carrier frequency of the receiver-received signal all change from time to time. Signal tracking means that the receiver should accurately always track these signal parameters. As shown in the figure, the tracking loop of the receiver includes a code tracking loop and a carrier tracking loop. Carrier tracking loops often include frequency-locked loops (FLLs) and phase-locked loops (PLLs), and delay-locked loops (DLLs) are often used in code tracking loops. FLLs, PLLs, and DLLs are characterized by a feedback adjustment mechanism that continuously corrects the carrier frequency, phase, or code phase generated within it according to the input signal to track the input GPS signal.

As shown in Figure 6, when the GPS IF signal enters the tracking loop, the received IF signal is first mixed with the carrier copied by the receiver's carrier tracking loop, and the carrier stripping is carried out to produce two data, in-phase (I) and quadrature (Q). Then, the code tracking loop will generate three C/A codes with a phase interval of d/2 in the lead (E), instant (P), and lag (L), which are correlated with the I/Q signal to obtain a six-way integration output. Among them, the recurrence codes generated by the leading branch, the immediate branch, and the lagging branch can be called the early code, the instant code, and the late code, respectively. Subsequently, the correlation integral values of the leading and lagging branches will be input to the code ring discriminator, and the correlation values of the instant branches will be input to the carrier ring discriminator. The phase and frequency errors are then calculated by different discrimination algorithms so that the carrier frequency, phase, and code phase reproduced in the tracking loop are corrected. The following is a detailed analysis of the impact of spoofing signals on PLLs and DLLs.

When there is no spoofing, the received signal contains a real satellite signal, and the correlation function between the real signal pseudocode and the locally reproduced pseudocode can be expressed as Equation 5 [31]:

$$R_a(t,\tau) = 1 - |\tau|, |\tau| \le 1\,(0, \text{others}), \tag{5}$$

where τ represents the code phase difference between the real signal t and the locally reproduced signal. After the signal enters the tracking loop, the real signal received after the carrier stripping and correlation operation will obtain the output result of the six-way correlator, which can be expressed as Equations 6–11 [31]:

$$I_E(t) = \sqrt{P_a} R_a\left(\Delta\tau - \frac{d}{2}\right)\cos(\phi_a), \tag{6}$$

$$Q_E(t) = \sqrt{P_a} R_a\left(\Delta\tau - \frac{d}{2}\right)\sin(\phi_a), \tag{7}$$

$$I_p(t) = \sqrt{P_a} R_a(\Delta\tau)\cos(\phi_a), \tag{8}$$

$$Q_p(t) = \sqrt{P_a} R_a(\Delta\tau)\sin(\phi_a), \tag{9}$$

$$I_L(t) = \sqrt{P_a} R_a\left(\Delta\tau + \frac{d}{2}\right)\cos(\phi_a), \tag{10}$$

$$Q_L(t) = \sqrt{P_a} R_a\left(\Delta\tau + \frac{d}{2}\right)\sin(\phi_a), \tag{11}$$

where P_a indicates signal power, $R_a(\cdot)$ represents a correlation function, $\Delta\tau$ represents the code phase difference between the received signal and the locally copied signal, and φ_a represents the carrier-phase difference between the received signal and the locally copied signal. When there is induced spoofing interference, the received signal contains a real signal and a spoofing signal, and after the real signal pseudocode is correlated with the local reproduction pseudocode, taking the real-time code as an example, the outputs of the I and Q correlators are as follows Equations 12, 13 [31, 32]:

$$I_p(t) = \sqrt{P_a(t)}R_a(t,\tau)\sin c(\Delta f_{d,a}T)\cos(\varphi_a) + \sqrt{P_s(t)}R_s(t,\tau)\sin c(\Delta f_{d,s}T)\cos(\varphi_s), \quad (12)$$

$$Q_p(t) = \sqrt{P_a(t)}R_a(t,\tau)\sin c(\Delta f_{d,a}T)\sin(\varphi_a) + \sqrt{P_s(t)}R_s(t,\tau)\sin c(\Delta f_{d,s}T)\sin(\varphi_s), \quad (13)$$

where $P_a(t)$ and $P_s(t)$ represent the power of the real signal and the spoofing signal, and $R_a(t,\tau)$ and $R_s(t,\tau)$ represent the correlation functions between the real signal pseudocode and the spoofed signal and the local pseudocode. $\Delta f_{d,a}$ and $\Delta f_{d,s}$ represent the carrier frequency difference between the real and spoofed signals and the local signal, respectively; φ_a and φ_s are the carrier-phase difference between the real and spoofed signals and the local signal, respectively. First, the output result of the instant branch correlator is sent to the PLL discriminator, assuming that the arctangent function phase discriminator is used, as shown in the formula $\Delta\hat{\varphi} = \arctan(Q_p/I_p)$. If there is no spoofing signal, the output of the phase detector is Equation 14 [31]:

$$\Delta\hat{\varphi} = \arctan\left(\frac{\sqrt{P}R_a(\Delta\tau)\sin(\Delta\varphi_a)}{\sqrt{P}R_a(\Delta\tau)\cos(\Delta\varphi_a)}\right) = \Delta\varphi_a. \quad (14)$$

At this time, the output result of the phase detector is that the phase deviation between the real signal and the local signal is $\Delta\varphi_a$. The PLL can then correct the local signal accordingly so that the carrier phase of the received signal can be continuously tracked.

However, when a spoofing signal is present, the output of the phase detector is Equation 15 [32]:

$$\Delta\hat{\varphi} = \arctan\left(\frac{\sqrt{P_a(t)}R_a(t,\tau)\sin c(\Delta f_{d,a}T)\sin(\varphi_a) + \sqrt{P_s(t)}R_s(t,\tau)\sin c(\Delta f_{d,s}T)\sin(\varphi_s)}{\sqrt{P_a(t)}R_a(t,\tau)\sin c(\Delta f_{d,a}T)\cos(\varphi_a) + \sqrt{P_s(t)}R_s(t,\tau)\sin c(\Delta f_{d,s}T)\cos(\varphi_s)}\right). \quad (15)$$

From this formula, when there is a spoofed signal, the phase identification result of the phase detector will be incorrect, and the PLL will not be able to correct the carrier phase of the local signal according to the phase identification result so that the carrier phase of the real signal cannot be tracked. Similarly, in the case of DLL, it is assumed that the DLL uses an incoherent leading hysteresis power phase detector. When there is no spoofing signal, the phase detector result is Equation 16 [32]:

$$\varepsilon = \frac{1}{2}\left[\left(I_E^2 + Q_E^2\right) - \left(I_E^2 + Q_E^2\right)\right] = \frac{p_a}{2}\left[R^2\left(\Delta\tau - \frac{d}{2}\right) - R^2\left(\Delta\tau + \frac{d}{2}\right)\right]. \quad (16)$$

Because the autocorrelation function of the pseudocode is symmetrical, $R(\Delta\tau - \frac{d}{2}) = R(\Delta\tau + \frac{d}{2})$. So, when the DLL keeps track of the received signal, $\varepsilon = 0$.

When there is a spoofing signal, it is not difficult to conclude that the correlation function between the received signal and the local copy code will be distorted to different degrees, and the code phase deviation of the spoofed signal relative to the real signal will lead to the asymmetry of the relevant peaks, thus causing the phase discrimination error of the DLL phase discriminator. For the sake of simplicity, if the PLL has tracked the carrier phase of the received signal at this time, the output result of this DLL phase detector is Equation 17 [32]:

$$\varepsilon = \frac{p_s}{2}\left[R\left(\Delta\tau - \frac{d}{2}\right) - R\left(\Delta\tau + \frac{d}{2}\right)\right] + \frac{P\cdot P_s}{4}\left[R\left(\Delta\tau_s - \frac{d}{2}\right) - R\left(\Delta\tau_s + \frac{d}{2}\right)\right], \quad (17)$$

where $\Delta\tau_s$ is the phase difference between the spoofed signal and the real signal number.

In conjunction with GNSS positioning principles, errors in the DLL and PLL discriminator tracking results can lead to inaccurate estimations of the code phase, carrier Doppler, and carrier phase of the received signal. This, in turn, introduces bias in the subsequent user position calculation, resulting in erroneous position and/or time information. However, the tracking loop also incorporates protective mechanisms. When the tracking loop is in a locked state and stably tracks the received satellite signal, it is in a tracking state. When the received signal fails to meet the tracking conditions, the tracking loop will cease operation, indicating a tracking loop loss of lock. This can lead to the receiver ceasing operation or attempting to reacquire the satellite. Such a scenario would be easily detectable and not conducive to covert spoofing. Therefore, spoofed signals must strive to avoid triggering a tracking loop loss of lock while gradually gaining control over the tracking loop to ensure it continuously tracks the spoofed signal. Ultimately, this will result in the receiver being misled by the spoofed signal.

3.2.2 Synchronous-induced spoofing model

Leveraging the receiver's inherent inclination to prioritize signals with greater power levels, the synchronous-induced spoofing model operates as follows: Once the receiver has acquired the authentic signal, the spoofing jamming platform utilizes the decoded code phase of the authentic signal to generate a spoofed signal with an identical code phase. This ensures that the authentic signal and the spoofed signal align at their correlation peaks. Subsequently, the spoofing jamming platform increases its transmission power to achieve a power advantage over the authentic signal, thereby causing the receiver to switch its tracking to the spoofed signal. The code phase of the spoofed signal is then gradually shifted away from the code phase of the authentic signal, effectively decoupling the receiver from the authentic signal.

Based on the correlation peak shown in Figure 7A, the general steps involved in the synchronous-induced spoofing model can be outlined [33].

(1) Initialization: The navigation receiver initially tracks the genuine signal. The spoofing jamming platform accurately estimates the parameters of the genuine signal upon its arrival at the receiver, including its code phase, carrier frequency, and signal power. Subsequently, a spoofed signal with a code phase aligned with the genuine signal is transmitted. At this stage, the power of the spoofed signal is lower than that of the genuine signal.

(2) Power enhancement: The power of the spoofed signal is gradually increased until it surpasses the power of the genuine signal. Upon achieving a power advantage, the target receiver loses lock on the genuine signal and re-locks onto the spoofed signal. The code loop and carrier loop begin to track the spoofed signal.

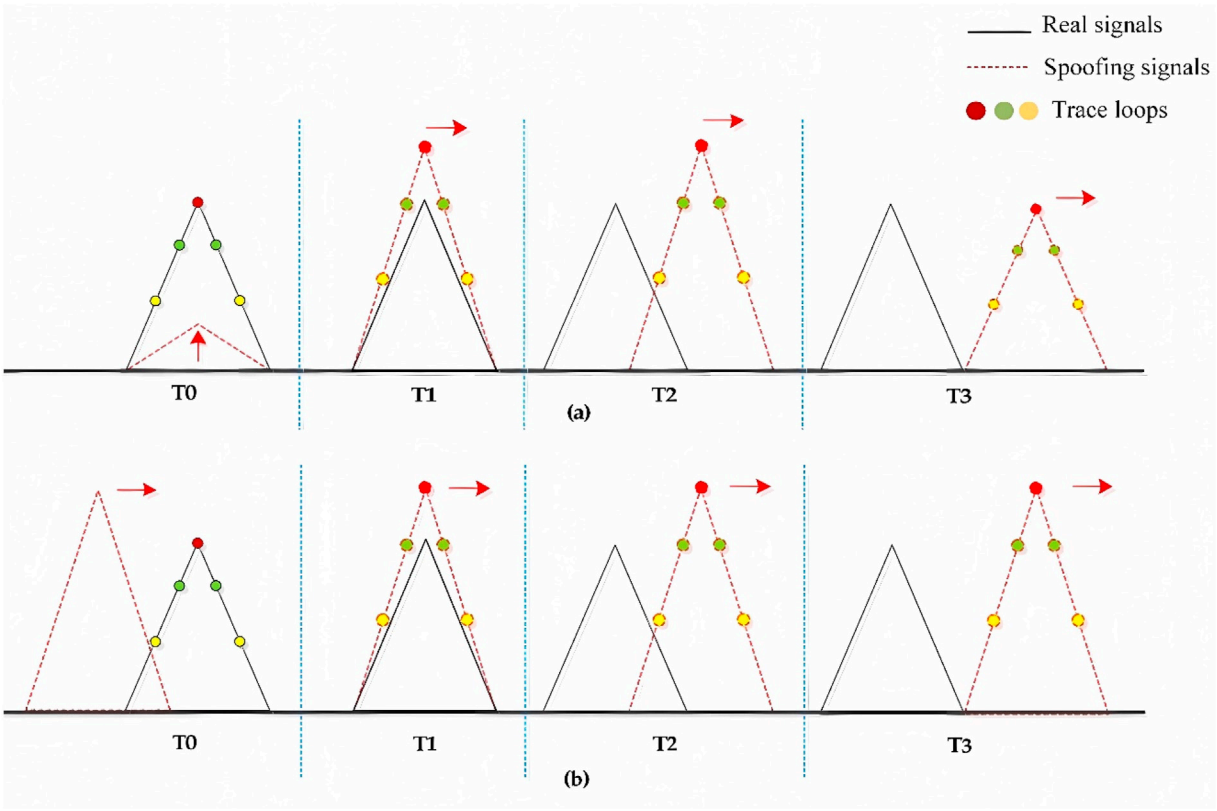

FIGURE 7
Schematic diagram of the changes of related peaks in the synchronous induction model and the asynchronous induction model.

(3) Code phase shift: Once the receiver is tracking the spoofed signal, its pseudo-random code rate is gradually adjusted, causing a shift in its code phase away from the code phase of the genuine signal. The target receiver then completely loses lock on the genuine signal, and the spoofed signal gradually replaces it entirely, effectively deceiving the receiver.
(4) Power reduction and completion: The transmission power of the spoofed signal is reduced to match the power level of the genuine signal, minimizing detection while completing the synchronous-induced spoofing process.

3.2.3 Asynchronous-induced spoofing model

While synchronous-induced spoofing models require precise alignment of the spoofed signal's code phase with that of the genuine signal, practical implementation faces challenges due to inherent inaccuracies in range and velocity measurements by the target receiver. The precision of parameter estimation, particularly for code phase, carrier frequency, and their respective compensations, often falls short of the requirements for synchronous induction. This presents significant hurdles in achieving synchronous spoofing. An asynchronous-induced spoofing model can be built on the synchronous-induced model. This model only necessitates a rough alignment between the code phase of the spoofed signal and the genuine signal. The spoofed signal then employs variable code rates to match the code phase of the genuine signal, enabling the tracking loop to lock onto the spoofed signal. The asynchronous-induced spoofing model presents a less challenging implementation than its synchronous counterpart. The correlation peak shown in Figure 7B illustrates the process.

Based on the correlation peak variations, the asynchronous-induced spoofing model can be divided into four steps [33].

(1) Initialization: The navigation receiver initially tracks the genuine signal. The spoofing jamming platform accurately estimates the parameters of the genuine signal upon its arrival at the receiver, including its code phase, carrier frequency, and signal power. Subsequently, a spoofed signal with a code phase slightly lagging the genuine signal is transmitted. Meanwhile, the spoofed signal maintains a power advantage over the genuine signal.
(2) Code phase matching: The code rate of the spoofed signal is gradually adjusted to bring its code phase closer to that of the genuine signal. When the two code phases align, the code loop, relying on the power advantage of the spoofed signal, tracks the spoofed signal, thus successfully disrupting the target receiver.
(3) Code phase shift: Once the receiver is tracking the spoofed signal, its pseudo-random code rate is gradually adjusted again, causing a shift in its code phase away from the code phase of the genuine signal. The target receiver then completely loses its lock on the genuine signal, and the spoofed signal gradually replaces it entirely, effectively deceiving the receiver.

TABLE 2 Characteristics of different methods of deception.

Types of spoofing	Forwarding spoofing attack	Generating spoofing attack	
		Synchronous-induced spoofing	Asynchronous-induced spoofing
How it works	Relays real satellite signals to increase latency and appropriate power for spoofing attacks	Imitate a satellite signal, increase the power from the same code phase, and then slowly change the code phase so that the receiver tracks the spoofing signal	Imitate the satellite signal, gradually approach the real signal number phase from the place where the code phase is different, and when the signal overlaps, increase the power and gradually increase the code phase so that the receiver tracks the deceptive signal
Merit	There is no need to know the specific parameters of the signal, and the implementation is simple	It is highly concealed, has a good deception effect, and is not easily detected by the receiver	It is highly concealed, has a good deception effect, and does not need to know the exact phase of the real letter number
Limitations	Latency alone is easy to detect.	The implementation is complex and also requires a relatively accurate analysis of the real signal. Because the military code data are not public, it is impossible to replicate the military signal	The implementation is complex and also requires a more accurate analysis of the real signal. Because the military code data are not public, it is impossible to replicate the military signal

(4) Power reduction and completion: The transmission power of the spoofed signal is reduced to match the power level of the genuine signal, along with adjustments to other parameters, minimizing detection while completing the asynchronous-induced spoofing process.

3.3 Summary

All the deception models mentioned above, as well as their applicable scenarios, advantages, disadvantages, and limitations, are shown in Table 2.

4 GNSS anti-spoofing jamming technology

In recent years, significant progress has been made in the development of spoofing interference countermeasure techniques, with numerous constructive solutions proposed by researchers from various countries. Current mainstream methods include signal power detection [34–37], time-of-arrival analysis [38], carrier and code phase consistency [39], carrier Doppler analysis [40], clock difference and stability analysis [41], signal arrival angle [42, 43], message verification [44], correlator output statistical characteristics [45], signal quality detection [46], signal spatial correlation [47], positioning results [48, 49], inertial navigation assistance [50, 51], and array antenna nulling techniques [52]. With the rapid development of machine learning, spoofing interference countermeasure methods can also be integrated with machine learning. Machine learning-based spoofing interference detection methods utilize the receiver to generate different types of feature values for spoofing identification. The type of signal can be detected by extracting these features, especially when the correlation peak of the spoofing signal is close to the original signal's correlation peak. Based on the implementation objectives, spoofing interference countermeasures can be broadly classified into four categories: spoofing interference detection and identification, spoofing interference suppression, and spoofing interference source localization.

4.1 Spoofing interference detection and identification

Spoofing interference detection and identification primarily focus on the detection of spoofed signals. Upon detecting the presence of such signals, the receiver's normal operation is halted, preventing it from being misled and mitigating potentially severe consequences. In a battlefield scenario, for instance, this would involve suspending the use of the receiver to prevent accidental weapon activation. However, spoofing interference detection alone is insufficient to effectively eliminate the spoofing interference and restore the receiver system to its normal operating state; further actions are required. The detection of spoofed signals is typically performed at the signal level without requiring modifications to the signal architecture, resulting in a straightforward implementation. Based on the implementation approach, various methods can be employed: (1) signal power detection, (2) correlation peak detection, (3) antenna array detection, (4) signal Doppler detection, (5) signal quality monitoring (SQM), (6) deep learning-based interference monitoring and identification, and (7) other methods of anti-spoofing interference.

4.1.1 Signal power detection

Satellite signals arriving at the ground typically exhibit very low power levels due to atmospheric attenuation caused by the troposphere and ionosphere, as well as multipath propagation. These signals are often masked by noise. Consequently, received navigation signals have relatively low power. The introduction of spoofing signals further exacerbates this issue, leading to a significant change in the receiver's signal-to-noise ratio, as illustrated in Figure 8. However, to effectively achieve their interference objectives, spoofing signal perpetrators typically transmit spoofed signals with slightly higher power than authentic signals. The signal power detection technique exploits this principle by establishing a reasonable detection threshold to identify the presence of spoofed signals within the receiver channel [53]. In 2012, Dehghanian V [36] proposed an effective detection method based on signal power. This method utilizes the output signal power of the correlator following signal acquisition and tracking to detect spoofing interference. It leverages the principle

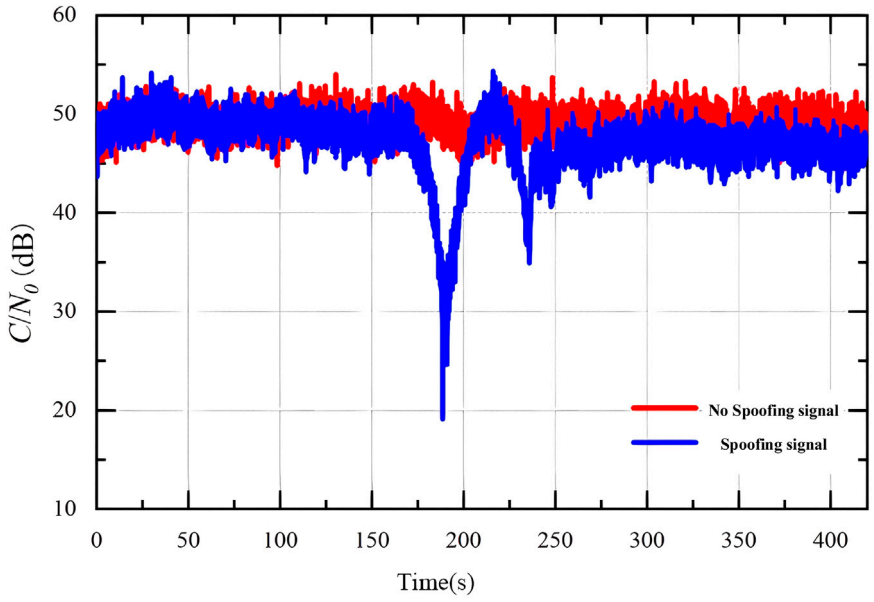

FIGURE 8
Noise floor change before and after adding the spoofing signal.

that spoofed signals typically exhibit higher power levels than genuine signals. A power threshold is established, and signals exceeding this threshold are classified as spoofed signals, while those below are considered legitimate. However, determining the appropriate spoofing interference judgment threshold for this method poses a challenge, particularly for induced spoofing interference, which can autonomously adjust its power level. This poses a significant risk of misclassification and potentially severe consequences. This algorithm requires no modifications to the receiver structure, rendering it simple to implement. However, its detection performance is compromised when the spoofed signal power is close to that of the BeiDou signal.

In 2016, [54] proposed a spoofing interference detection algorithm based on signal-to-noise ratio (SNR) measurement. This algorithm exploits the high SNR anomaly generated during spoofing signal intrusion to identify spoofed signals based on correlator peak values. While simple to implement, this method demonstrates limited effectiveness against highly concealed induced spoofing interference. In 2018, Wesson K. D. et al. [55] proposed a spoofing interference detection technique called the power distortion detector. This technique categorizes received signals as interference-free, multipath interference, or spoofing interference based on observations of received signal power and correlator function distortions. This technique effectively differentiates low-power spoofed signals from multipath signals and requires no modifications to the receiver hardware, making it straightforward to implement.

In 2019, [56] investigated the detection statistics of power detection methods based on the principles of power detection techniques and provided specific detection thresholds. In the same year, [57], recognizing the limitations of the carrier-to-noise ratio (CNR) detection algorithm, proposed a spoofing interference detection algorithm that combines the CNR algorithm with the Doppler detection algorithm during the signal tracking phase. This approach overcomes the shortcomings of relying solely on the CNR algorithm for spoofing detection. In 2020, [58], acknowledging the limitations of using solely signal power to detect spoofing interference, proposed a spoofing interference detection algorithm based on power changes for mobile terminals. This algorithm leverages the distinct power variations exhibited by spoofed and genuine signals at the same distance when the terminal is in motion to make spoofing interference judgments. This algorithm demonstrates superior performance when the interference source is less than 2000 m from the terminal, and the terminal's movement distance exceeds 200 m, but it also possesses certain limitations.

4.1.2 Correlation peak detection

Correlation peak detection techniques have demonstrated remarkable effectiveness in detecting forwarding-based spoofing interference. This effectiveness stems from the inherent time delay present in forwarded spoofing signals compared to genuine signals. This time delay inevitably results in a greater transmission distance and time for the spoofing signal to reach the target receiver than the genuine signal. Consequently, the received signal exhibits anomalous correlation peaks during the acquisition or tracking stages. The associated peak anomalies are shown in Figure 9.

In 2016, [59] proposed a detection algorithm that combines correlation peak and power analysis for forwarding-based spoofing interference. This algorithm determines the presence of spoofing interference by analyzing the number of correlation peaks exceeding the acquisition threshold and setting appropriate power detection thresholds. While simple and effective, it suffers from detection blind zones. Building upon Wang Zhiying's work, [60] introduced the full width half maxima (FWHM) algorithm as a supplementary approach to the multi-peak algorithm for detecting short-delay forwarding-based spoofing interference. This algorithm, which requires no modification to the receiver structure, offers

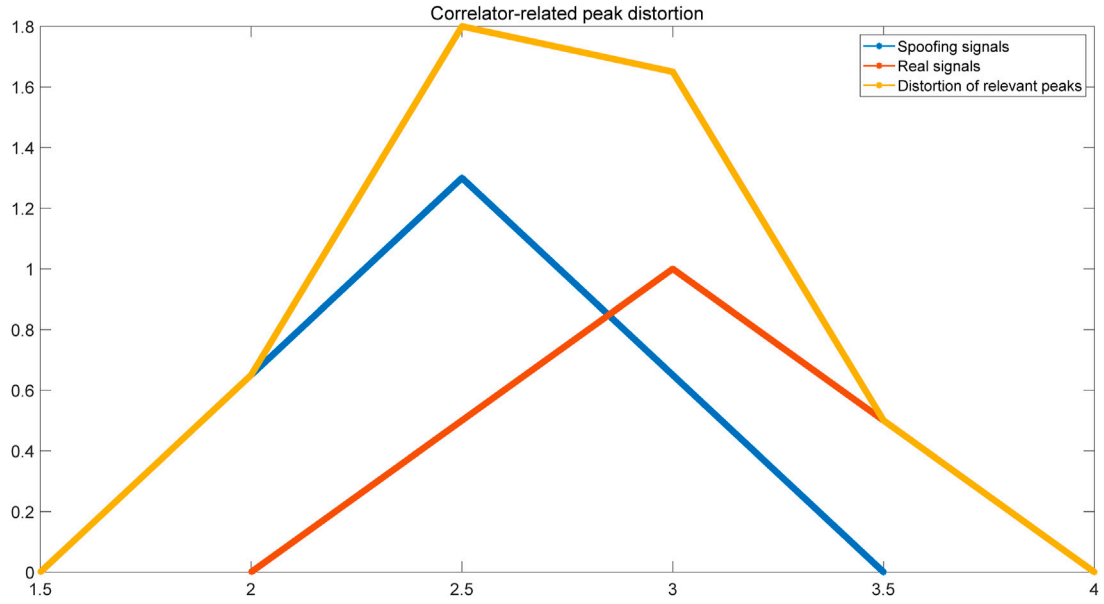

FIGURE 9
Schematic diagram of peak changes related to ultra-low delay.

simplicity in implementation. However, it cannot effectively distinguish between spoofing signals and multipath signals. To address the shortcomings of the algorithms, [61] proposed a novel joint detection algorithm for the acquisition stage in 2021. This algorithm extends the previous two approaches by incorporating a code phase difference consistency method, effectively mitigating the influence of multipath signals. It further refines the correlation function width threshold method [62], thereby addressing the limitations of the previous algorithms. This enhanced algorithm exhibits robust detection capabilities, successfully detecting forwarding-based spoofing interference with varying time delays.

The analysis presented above clearly demonstrates the efficacy of correlation peak detection techniques in detecting forwarding-based spoofing interference during the signal acquisition stage. Consequently, this research will delve into signal correlation peak detection techniques, exploring their integration with signal power detection techniques to detect forwarding-based spoofing interference. In 2022, [63] designed a receiver scheme incorporating interference identification capabilities. This scheme leverages the distinct correlation peak shapes generated by different types of interference, employing deep learning to recognize and classify these feature maps.

4.1.3 Antenna array detection

Array antenna detection techniques leverage the spatial characteristics of spoofing signals and BeiDou signals to identify the presence of interference. Due to implementation constraints, spoofing signals currently received by array antennas typically originate from a single direction [64, 65], while satellite signals arrive from multiple directions. These detection techniques demonstrate excellent performance but often require additional hardware implementation, resulting in high algorithmic costs.

In 2016, [66] proposed an algorithm for spoofing signal detection using the carrier-phase difference between two antennas. This algorithm utilizes the precise location of the tracked satellite as prior information to determine the carrier-phase difference of the true signal on the known antenna array. It further analyzes various error sources in the carrier-phase difference calculation to detect spoofing signals. This algorithm exhibits superior detection performance when the baseline of the antenna array is longer and the incident azimuth angle is smaller. However, it has limitations, as it is suitable for navigation receivers with fixed antenna installations. In 2018, [67] proposed a blind adaptive array signal processing method based on array antennas. This method not only adaptively forms deep nulls in non-periodic, periodic, and generative spoofing interference direction of arrival (DOA) estimation but also mitigates in-band spoofing signals and enhances the useful signal. In the same year, [68] proposed a spoofing interference detection method based on baseline data statistical analysis. This method considers three scenarios: single fixed baseline, fixed independent baseline, and dual independent baseline models. It analyzes the impact of baseline values on detection performance. However, this method may fail when the two antennas are not synchronized. Addressing this issue, [69] proposed a pseudo-range and carrier-phase measurement asynchronous model and spoofing interference detection method based on dual antenna power measurements. This method can detect spoofing interference under asynchronous conditions. Furthermore, many researchers [70, 71] have proposed corresponding multi-antenna spoofing interference detection techniques. In 2019, [72] proposed a blind detection method for spoofing signals using antenna array spatial diversity. This method is implemented in a snapshot receiver and evaluated using open data recorded by a six-element array. It exhibits a high detection rate but has high complexity. To address the challenge of detecting spoofing

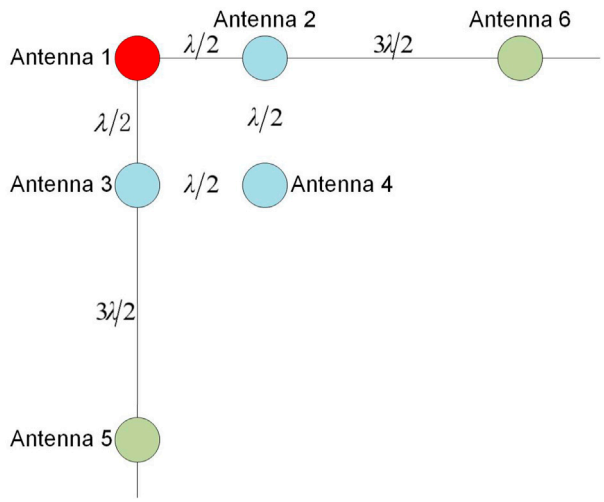

FIGURE 10
Schematic diagram of the arrangement of six array elements antenna elements [77].

signals from different emitters, [73] proposed an anti-spoofing method. This method uses pseudo-range double differences (PRDD) measurements from two receivers to detect this type of spoofing interference. Spoofing signals are identified by analyzing the difference between PRDD measurements and estimated PRDD values. This algorithm exhibits good detection performance when the two receivers are placed at an appropriate distance. However, it may fail if the platform is too small. In 2020, [74] proposed an algorithm for detecting spoofing interference using carrier-phase single difference (CPSD) measurements from a linear array. Compared to the method in [73], this algorithm has less stringent platform size requirements and can be applied to a wider range of scenarios.

In 2021, [75] addressed the limitation of traditional spoofing interference detection algorithms, which are unable to locate spoofing interference. They proposed a spoofing interference detection method based on carrier-phase difference measurement using array multi-antenna received signals. This method can estimate the arrival direction of the received signal using the direction-finding principle of the correlation interferometer without requiring prior knowledge. Spoofing interference can be determined by comparing this estimate with the satellite direction obtained from ephemeris calculations. This algorithm exhibits excellent detection performance and can identify the arrival direction of multiple spoofing signals from different satellites. However, it has high algorithmic complexity. In 2022, Wang Xiaoyu [76] utilized the difference between real satellite navigation signals, which arrive at the array antenna from multiple directions in the upper hemisphere space, and spoofing interference signals, which arrive from a single direction. The MUSIC algorithm is used to estimate the incident direction of each satellite, and spatial consistency is employed for spoofing interference determination. This algorithm has good detection performance but has high computational complexity due to the need to measure the arrival direction of each satellite.

In 2023, [77] proposed a novel six-element array spoofing interference detection array antenna, as shown in Figure 10. Spoofing interference can be detected and identified by monitoring the relevant peak values and combining spatial capture algorithms. Additionally, they used the long and short baseline algorithm to quickly search the entire cycle ambiguity, enabling high-precision detection of spoofing interference sources. This method exhibits high detection accuracy but requires many antenna elements, leading to higher costs.

4.1.4 Signal Doppler detection technology

For single-antenna spoofing interference, the Doppler data dispersion between two real satellite signals exhibits non-linearity in the time domain when the receiver is moving randomly. Conversely, the Doppler data dispersion between two single-antenna spoofing signals displays linearity. Additionally, the Doppler frequency shift range of the satellite signals received by the target receiver expands when spoofing interference is present. Therefore, monitoring Doppler frequency shift variations can effectively identify the presence of spoofing interference. Figure 11 shows the nominal recorded carrier frequency error for the four space vehicles (SVs) used in this article. As expected, the carrier frequency of each SV varies approximately linearly with time. The longer the transmission time, the greater the offset of the SV from the original carrier frequency. The slope of the line correlates with the expected Doppler shift of approximately ±5 kHz modeled in this study.

In 2014, [78] proposed an adaptive tracking algorithm for forwarding-based spoofing interference, combining a power threshold detector with a Doppler frequency shift detector. This algorithm is suitable for forwarding-based spoofing interference but less effective against other types. In 2018, [79] presented a GNSS anti-spoofing algorithm based on Doppler frequency shift. This algorithm derives a Doppler frequency difference model and transforms the spoofing interference detection problem into a sequence linear detection problem. While simple, effective, and demonstrating good detection performance, this algorithm may exhibit reduced effectiveness against more sophisticated spoofing interference. [82] proposed a joint detection of code and carrier Doppler that can detect and identify spoofing signals. This method is implemented on the GNSS acquisition module and requires no additional hardware. It exhibits good detection performance in static and uniform motion scenarios, but the detection effect is inferior when the receiver's acceleration is significant. In the same year, [83] proposed a spoofing interference detection algorithm based on the consistency of Doppler positioning repair and pseudo-range positioning repair. The algorithm effectively improves the performance of Doppler positioning methods and detection methods through an improved Doppler smoothing technique based on alpha filtering. In 2019, [80] proposed a spoofing interference detection algorithm for medium-level spoofing interference based on frequency-domain double peaks and relative velocity residuals. This technique employs a fast Fourier transform (FFT)-based approach to detect double peaks and extract their Doppler difference. It then calculates the relative velocity residuals based on the Doppler difference. This algorithm not only detects spoofing signals but also distinguishes them from multipath signals. In the same year, [81] proposed a detection

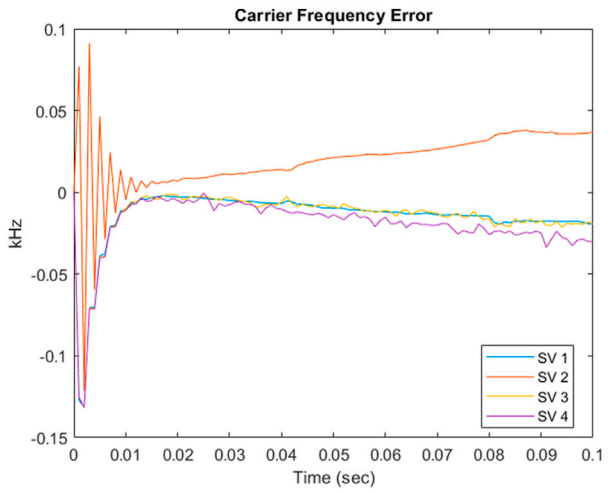

FIGURE 11
Carrier frequency error due to Doppler shift [85].

method that jointly utilizes the carrier Doppler frequency shift caused by the vertical reciprocating motion of the receiving antenna and the navigation information conveyed by the received signal. [84] proposed a spoofing detection method that utilizes the amplitude difference and frequency difference between the superposition composite signal containing interference and the normal signal unaffected by spoofing in the tracking loop as the basis for interference detection. This method can effectively detect spoofing signals in BeiDou satellite navigation signals by setting signal power anomaly thresholds and Doppler frequency shift detection thresholds. In 2022, [85] proposed a spoofing interference detection technique based on Doppler frequency difference correlation. This method calculates the Fréchet distance between two satellites by using the least-squares fitting of Doppler measurements within a window when the receiver is moving. After obtaining the similarity evaluation value between them, it is used to detect spoofing interference. This method has low computational complexity and requires less additional information, but its application scenarios are limited. In 2024, [86] proposed an unmanned aerial vehicle (UAV) GNSS spoofing detection method based on signal characteristics: Doppler frequency shift carrier-to-noise ratio density and deep learning. After training, the detection probability can reach 95%.

4.1.5 Signal quality monitoring (SQM)

Signal quality monitoring (SQM) technology is widely employed in satellite navigation systems. The advantage of SQM lies in its simple structure, enabling the detection of spoofing interference without altering the receiver's original design. This is achieved by analyzing the correlator output peaks of the satellite navigation receiver. Typically, the GNSS receiver correlator output exhibits a characteristic red inverted triangle shape, as depicted in Figure 7. The early code correlator output and the late code correlator output are always symmetrical with respect to the prompt code correlator output. When the correlator spacing is 0.5 chips, the prompt code correlator output is twice the sum of the early code correlator output and the late code correlator output at the same time. In the presence of interference, the outputs of the early code, prompt code, and late code correlators become abnormal, and their symmetry is disrupted. For example, under normal circumstances, the output power of the early code and the late code should be equal, ideally zero, but after the injection of deception, the output power difference between the early code and the late code will exhibit a significant abnormal change, as shown in Figure 12.

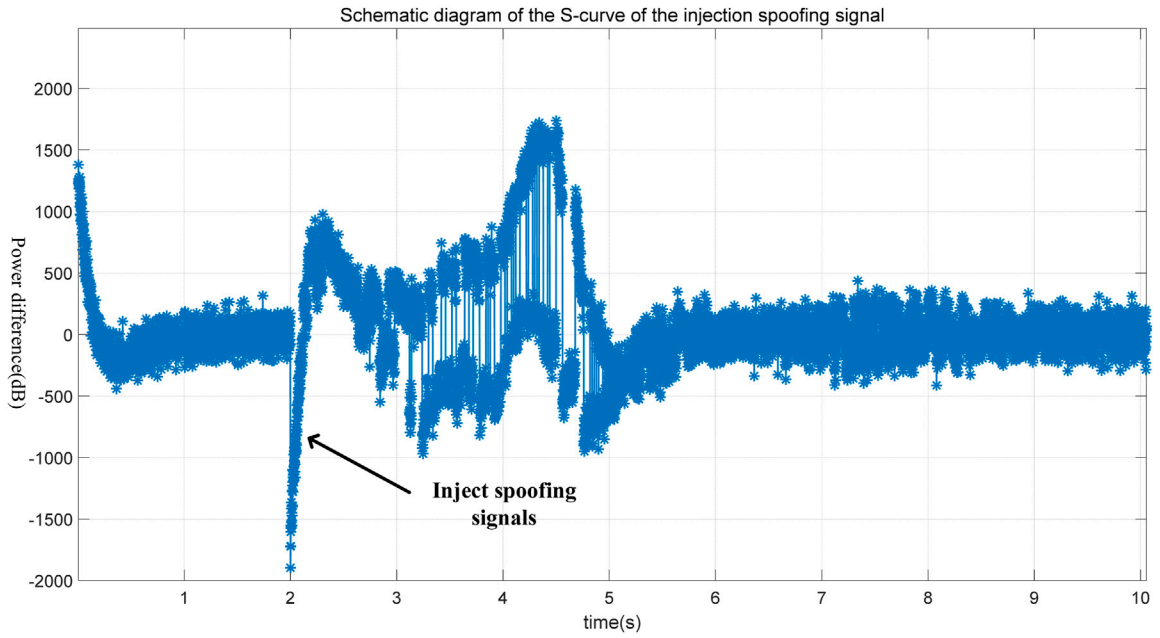

FIGURE 12
Schematic diagram of the change of early code power and late code power.

Numerous algorithms have emerged from SQM. [87] introduced the delta metric (detecting correlation peak distortion by comparing the in-phase outputs of the early and late code) and the ratio metric (detecting correlation peak distortion by observing the ratio of early and late codes to the prompt code in-phase outputs). Subsequently, [88] proposed the S-curve-bias (SCB) algorithm. Induced spoofing interference can affect the correlator output. This algorithm utilizes the difference between the outputs of the early code correlator and the late code correlator to detect induced spoofing interference. [89] introduced a joint metric approach for SQM, constructing a joint detection metric based on code delay and carrier phase to enhance detection algorithm performance. Prisiavash et al. [90] presented a two-dimensional SQM detection algorithm based on code delay and Doppler frequency. While this algorithm improves detection performance, it significantly increases computational complexity. [91] applied sliding window variance and sliding window averaging to existing SQM methods, significantly improving detection performance in static spoofing interference environments. [92] applied sliding window variance processing to the SCB method and proposed a detection algorithm based on SCB variance.

The target receiver obtains the corresponding code phase value through the zero-crossing point of the code discriminator curve (i.e., the S-curve) in the code tracking loop. In the absence of interference and noise, the code phase value corresponding to the zero-crossing point of the S-curve is zero. However, due to the channel transmission distortion and non-linear effects of power amplifiers, the code phase value fluctuates near zero. The SCB value, which measures the code tracking error, serves as a criterion for detecting spoofing attacks.

[93] proposed a method based on weighted second-order moments (WSCM) to detect induced spoofing interference, targeting the gradual dynamic adjustment process where spoofing and genuine signals interact during the tracking stage, leading to correlation peak symmetry distortion. Specifically, a weighted criterion for the time-domain transient response values of multiple correlators is established by expanding the second-order central moment (SCM) [94] of the navigation signal waveform. A WSCM test statistic is then constructed, accurately quantifying correlation peak symmetry. [95] combined radio power detection metrics with automatic gain control and C/N0 measurements, along with the multi-correlation of signal distortion, to construct new SQM thresholds for detecting and identifying spoofing interference. This method introduces a novel metric to SQM. This SQM metric requires additional correlators, which expands the investigation area but accurately identifies spoofing interference among various interference attacks.

[96] proposed a robust spoofing interference detection method for GNSS instruments using the Q-channel signal quality monitoring metric. This method utilizes and measures the abnormal energy in the Q-channel of the tracking loop for spoofing interference detection. This SQM metric overcomes the challenge of constantly changing relative carrier phases between real and spoofing signals, achieving higher detection probability while being cost-effective and highly practical. It only requires minimal modifications to the traditional receiver's baseband correlator and firmware. [97] proposed a spoofing detection algorithm based on a combination of SQM and tracking parameters. This method leverages the complementarity between different SQM metrics, proposing an "OR" rule that combines various SQM parameters and determines the corresponding optimal detection threshold. Compared to a single SQM measure, SQM measure fusion based on the "OR" principle exhibits significant performance improvements in detection. [98] proposed a spoofing detection algorithm based on a vector tracking structure using SQM. This method overcomes the limitation of traditional SQM algorithms, which become ineffective when correlation peaks do not overlap. It utilizes existing observations in tracking to detect spoofing attacks on the pseudocode and carrier. [99] addressed the low detection accuracy and susceptibility to the power advantage and carrier phase drift of spoofing signals in traditional SQM techniques. They proposed an innovative SQM method that employs the Kolmogorov–Smirnov (KS) test for detecting receiver correlator output. This method overcomes the performance limitations of traditional SQM techniques, effectively detecting subtle symmetry distortion of the correlation function and signal power changes caused by spoofing signals. It serves as a potential reliable application solution for spoofing attacks with different frequency locking modes and power consumption advantages. It also avoids changes to the receiver hardware structure and has low computational complexity.

4.1.6 Deep learning-based spoofing interference detection and identification

Given the rapid advancement of deep learning, its application in spoofing interference detection and identification has become inevitable. Deep learning approaches for interference signal detection and identification involve processing and analyzing received signals to isolate interference signals and determine their types and parameters. Interference signal identification typically involves analyzing signal characteristics such as feature parameters, time-domain characteristics, frequency-domain characteristics, and phase characteristics. Deep learning methods utilize signal feature parameters when spoofing is present and absent as network inputs for training, resulting in a network capable of rapidly distinguishing spoofing based on different features.

Preprocessing is usually required to identify the type of interference in the received signal. One such method is normalization or zero-mean normalization [100], transforming the signal into a standard form to minimize differences. Signal feature parameters, such as power spectral density, frequency, amplitude, and phase, are extracted by analyzing the time-domain, frequency-domain, and phase characteristics of the signal. The type of interference signal can be determined by further analyzing these feature parameters, such as narrowband interference, broadband interference, or pulsed interference [101]. Common classification algorithms include decision trees (DT) [102, 103], support vector machines (SVM), and backpropagation (BP) neural networks [104, 105].

[106] investigated the types and methods of interference signals in satellite navigation systems. Time-domain cross-correlation features of the received signal were extracted, considering the localization and identification of multiple interference signals. The SVM was then used to classify and identify the interference signals. To enhance the system's noise resistance, a convolutional neural network (CNN) was used for interference signal recognition,

significantly improving recognition performance at low interference-to-noise ratios. A backpropagation neural network (BPNN) is a neural network model trained using the error backpropagation algorithm. It consists of an input layer, hidden layers, and an output layer, where hidden layers can have multiple layers. The BPNN algorithm computes the network's output value through forward propagation and then compares the output value with the actual value to calculate the error value. Next, the error value is backpropagated to the network, adjusting the weights of each layer to minimize the error. The key to the BPNN algorithm is the error backpropagation algorithm, which utilizes the chain rule to propagate errors from the output layer to the input layer, calculating the error of each layer and then adjusting the weights of each layer to minimize the error.

[107] investigated BPNN identification algorithms, but BPNN algorithms have issues, such as becoming stuck in local optima and slow training speed. In classification and recognition problems, decision trees classify input variables into a predefined category through a series of decision nodes. In regression problems, decision trees use a series of decision nodes to ultimately produce a continuous output value. The basic principle of decision tree classification algorithms is to construct a tree-like structure based on different values of input features, assigning different input samples to different categories. The process of constructing a decision tree can use recursive partitioning, and [108] designed a stable classifier using the decision tree approach. It was implemented and tested on a hardware platform. Residual networks (ResNet) are a type of deep neural network architecture that addresses the problem of training deep neural networks by introducing residual blocks. Residual networks allow information to propagate directly across layers, enabling deep networks to better capture the relationship between input and output, thus improving the efficiency and accuracy of training deep networks. [109] simulated and analyzed deep learning-based recognition algorithms by constructing real and complex residual networks with CNNs. The study found that the main advantage of a ResNet is that it can further improve the network performance by adding more layers while maintaining model accuracy. The gravitational search algorithm (GSA) is an optimization algorithm based on Newton's law of universal gravitation and Newton's second law, simulating the interaction between celestial bodies. It searches for the optimal solution by simulating parameters such as gravity, mass, and velocity. The basic idea of the algorithm is to view the optimization problem as a celestial system, where each solution is considered a celestial body, its mass being proportional to the fitness value and its position representing the parameters of the solution. During the search process, each solution is affected by the universal gravitational force and centripetal force of other solutions. The centripetal force moves the solution toward the direction of the historical optimal position, while gravity moves the solution toward a better position.

Based on the GSA algorithm, [110] optimized the parameters of SVM for identifying audio interference in terrestrial-to-space communication. Simulation results show that GSA has advantages such as being simple to implement, having a strong global search capability, and fast convergence speed. SVM is a binary classification algorithm, but it can be used for multi-class recognition through various methods. [111] used the one-vs.-all method for multi-class recognition. This algorithm has high recognition efficiency and high classification accuracy. [112] proposed a deep learning spoofing detection method based on representation learning. This method addresses the problem of deep learning methods being limited by training data and can be trained using a single dataset. This lightweight critic-model-based score detector can be seamlessly integrated into GNSS receivers through firmware updates once trained offline, thus reducing additional overhead.

4.1.7 Other methods of anti-spoofing interference

Beyond signal-level detection and identification of spoofing interference, techniques involving modification of signal structures, such as spread spectrum code encryption and message encryption, can also be employed for spoofing interference monitoring and identification. However, these approaches alter the GNSS signal structure, limiting their practical applicability. Simultaneously, anti-spoofing technologies combined with external auxiliary techniques are also emerging, such as integration with inertial navigation units, other radio navigation systems, and other sensors. Among these, the combination of a GNSS with inertial navigation units (INS) is the most widely used anti-spoofing approach. INS positioning solutions are unaffected by external interference, providing auxiliary information for the detection and suppression of GNSS spoofing interference. Existing INS/GNSS integrated navigation anti-spoofing techniques mainly include spoofing detection algorithms based on Kalman filter innovations and innovation rate [113, 114], spoofing detection algorithms based on the comparison of INS and GNSS raw measurements [115], and INS-assisted GNSS carrier-phase spoofing detection [116].

4.2 Spoofing interference suppression

Spoofing interference suppression aims to eliminate spoofed signals after detection and identification, thereby restoring the normal operation of the navigation system. The most prevalent approach for spoofing interference suppression is the use of array antenna nulling. This technique encompasses two methods: spatial [117] and spatiotemporal [118] processing. The core principle involves generating nulls in the direction of the interfering signal to suppress the interference. Array antenna nulling can be categorized into pre-despreading and post-despreading spoofing interference suppression. Pre-despreading methods have a smaller computational load and leverage the characteristic of spoofing interference power superposition in the spatial domain. They estimate the spoofing signal steering vector or signal subspace to achieve spoofing interference suppression. However, the suppression performance of this method is significantly affected by the spoofing signal power. Higher spoofing signal power generally leads to better interference suppression performance. Conversely, post-despreading spoofing interference suppression techniques first identify the spoofing interference signal and then calculate the steering vector and weights specifically for the spoofing signal.

Pre-despreading spoofing interference suppression methods typically leverage the power advantage of spoofing interference to

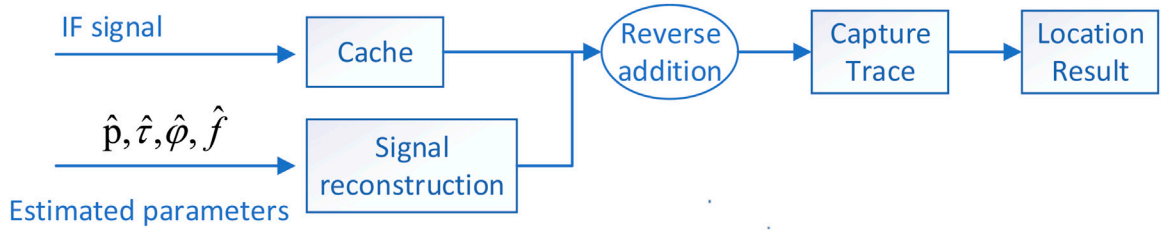

FIGURE 13
Block diagram of the signal reconstruction deception jamming suppression method.

estimate the steering vector and spatial information. Based on this information, weights are calculated for weighting, achieving spoofing interference suppression. However, the accuracy of spoofing interference spatial information estimation is significantly influenced by the power level due to the lower signal-to-noise ratio before despreading. The suppression performance deteriorates under low spoofing interference power conditions. Nonetheless, because despreading is not required, the computational load is smaller than post-despread interference suppression methods. Despreading improves the signal-to-noise ratio for post-despreading spoofing interference suppression methods, leading to more accurate signal spatial characteristics. It also allows for obtaining carrier phase information that can be used to identify spoofing signals based on other characteristics, further enabling interference suppression. In addition to these methods, signal reconstruction can be employed for spoofing interference suppression in single-antenna receivers, as illustrated in Figure 13. This approach involves detecting spoofing interference and extracting its code delay, Doppler frequency, carrier phase, and signal amplitude to reconstruct the spoofing signal. The reconstructed signal is then subtracted from the original intermediate frequency (IF) navigation signal, effectively eliminating the spoofing interference and yielding a spoofing-free navigation signal.

[119] proposed a spoofing signal classification module to distinguish between spoofed and genuine signals, reconstructing and eliminating the spoofed signal based on its characteristics. The processed signal is then re-examined, and if spoofing interference is detected, the process of reconstruction and elimination is repeated. [120] estimated the amplitude and phase of the spoofing signal to reconstruct it, subtracting the reconstructed signal from the delayed original signal. The performance was evaluated using the interference cancellation ratio (ICR). Simulation results from these studies indicate that signal reconstruction exhibits excellent suppression performance, but it necessitates continuous and accurate acquisition of spoofing signal information, leading to significant complexity and implementation challenges.

The difficulty and computational complexity of accurately estimating all parameters of spoofed signals significantly limit the application of signal reconstruction methods [121]. HANS et al. [122] proposed a subspace projection method that estimates the carrier frequency and code phase of spoofed signals through capture tracking. A signal subspace of the forged signal is constructed by exploiting the near orthogonality of their PRN codes. The received signal is then orthogonally projected onto this subspace, suppressing the spoofed signal and enabling the capture and tracking of the true signal. Compared with signal reconstruction methods, this method requires less information about the spoofed signal and exhibits better robustness. However, if the phase difference between the spoofed and true signals is less than one chip, the suppression function will be lost, indicating that this method cannot detect spoofed signals with small deviations.

[123] proposed an adaptive beamforming algorithm for spoofing interference suppression in GNSS receivers. Adaptive beamforming can control the radiation pattern of the antenna array, suppressing spoofed signals from the direction of the spoofing interference source and enhancing the true navigation signals from the direction of navigation satellites. Beamforming technology is used simultaneously with spoofing interference detection technology based on antenna arrays. First, baseband signals are acquired through the antenna array, and a circulant matrix is established. Spoofing interference detection is achieved based on eigenvalue testing. Subsequently, spoofing interference is suppressed, and the true signal is enhanced through beamforming technology. Adaptive beamforming has many applications in the suppression of jamming interference, and the algorithm is relatively mature. It can be directly applied to spoofing interference suppression and can simultaneously suppress both jamming and spoofing interference. However, with the increase in the number of interference directions, the antenna array needs to further increase the number of antenna elements, making the complexity and high cost of the equipment the main reasons limiting its widespread application. Introducing a multi-correlator structure in the receiver allows for simultaneous capture and tracking of both the true signal and spoofed signals. Subsequently, a decision method confirms the true signal and eliminates spoofed signals, enabling the detection and suppression of spoofing signals. When multiple signals exist in the received signal, multi-signal tracking is performed using multiple correlators without prior knowledge of the spoofed signal. The multipath estimating delay lock loop (MEDLL) technique is used to process the baseband signal, obtaining the signal's amplitude, propagation delay, and carrier phase, denoted as [124]. Subsequently, based on the estimated amplitude, propagation delay, and carrier phase of the signal, one set of signals is removed from the original baseband signal and tracked separately, thereby obtaining the tracking results of the other set of signals.

In combined navigation-based spoofing interference detection methods, if the satellite navigation receiver is determined to be

TABLE 3 Summary table of different spoofing interference suppression methods.

Method	Complexity	Performance	Limitations
Signal reconstruction	High	Medium	It is necessary to obtain spoofing signal information continuously and accurately
Subspace projection	Medium	High	Fails when the phase difference between the deception signal and the real signal is less than one chip
Beamforming	Medium	High	Requires array antennas with element spacing less than half the wavelength
Multi-correlator method	Low	Medium	It will fail when the amount of computation is large, and the power of the spoofing signal is large
Integrated navigation method	Medium	Medium	Requires additional hardware or sensors
Direct positioning method	Medium	Medium	Has poor performance at medium to low signal-to-noise ratios
Receiver autonomous integrity monitoring	Medium	Medium	Spoofing signal power is required, and there are multiple satellites

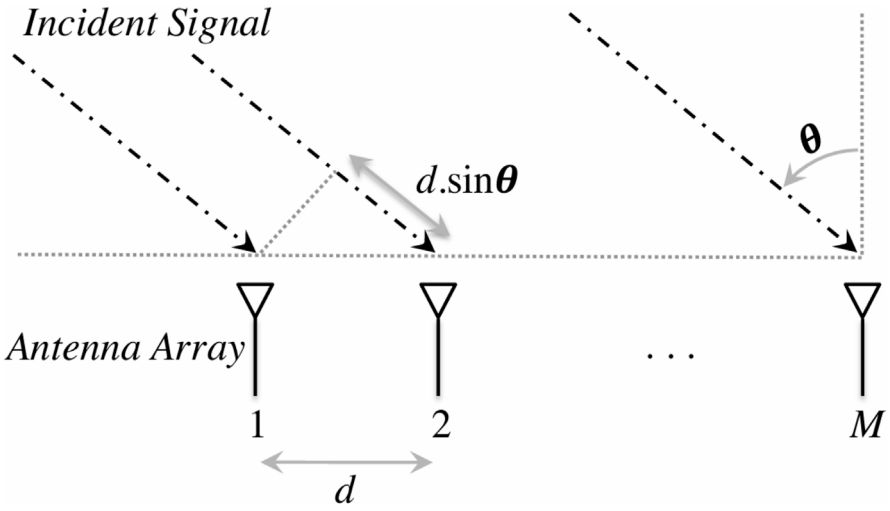

FIGURE 14
Schematic diagram of the signal angle of arrival measurement [125].

spoofed, non-satellite navigation systems are used for navigation, achieving spoofing interference suppression. The essence of this method is to discard untrustworthy satellite navigation results and select other reliable navigation results. The disadvantage of this method is that it requires multiple navigation systems, which increases costs. Moreover, the positioning accuracy after suppression depends on the performance of the other navigation methods.

Receiver autonomous integrity monitoring (RAIM) is also an effective spoofing interference suppression method. This method can effectively eliminate faulty satellites. In cases with fewer spoofing interference signals, they can be eliminated from the received signals, ensuring the authenticity and validity of the navigation positioning results. However, in general, to obtain reliable positioning solutions from the receiver, spoofing interference often requires the simultaneous transmission of false signals from multiple satellites with a higher power level than the true signal. This may lead to the receiver completely capturing and tracking the spoofed signal, rendering the RAIM algorithm ineffective. Table 3 below summarizes the complexity, performance, and limitations of various methods.

4.3 Spoofing interferer location

Detecting, identifying, and suppressing spoofing signals are challenging tasks, often requiring the addition and upgrade of receiving equipment, significantly increasing the cost of spoofing interference suppression. Another approach to spoofing interference suppression is to focus on high-precision strikes against the spoofing interference source, eliminating its impact by destroying it. Existing methods for locating satellite navigation spoofing sources employ a two-step localization approach. In the first step, the receiver intercepts the spoofing interference signals and performs initial signal processing to estimate parameters such as time of arrival (TOA), time difference of arrival (TDOA), frequency difference of arrival (FDOA), and angle of arrival (AOA). The second step establishes an equation relating these intermediate parameters to the spoofing source location, and solving this equation yields the location information. Angle of arrival (AOA) analysis based on antenna arrays is currently the most practical method for locating spoofing sources. The algorithm principle is illustrated in Figure 14. Given that spoofing sources are typically fixed, the direction of

TABLE 4 Positioning methods and receiver requirements.

Targeting method	Spoofing interference feature	Receiver requirements
Multi-receiver detection	Spoofing jamming is emitted by the same interferer	Multiple satellite nav receivers in different locations
Integrated navigation detection	Only one GNSS system is spoofed	Inertial navigation and satellite navigation combined
Clock error detection	The deception jamming clock is inconsistent with the real clock difference	——
Signal reconstruction (residual signal detection)	Real signals can be detected.	Multiple signal reception channels
Spoofing interferer location	Multiple spoofing signals come from the same interferer.	Multiple receivers in different locations
Message verification	Unencrypted	Encryption verification
Power detection	Absolute power detection	The receiver has a power detection function that can distinguish higher signal amplitudes
	Relative power detection	
	Automatic gain control (AGC) detection	The receiver is equipped with a carrier-to-noise ratio detection function
	Power rate of change detection	
Arrival time detection	There is a delay in spoofing signals	Arrival time analysis
Correlation detection	Multiple spoofing signals come from the same direction	Measure the correlation coefficient of the output of different tracking channels
Signal quality checking	The true signal-related peaks are distorted	Multiple correlators
Airspace/space-time detection	The on-road signal is coming from the same direction	Multiple receiving antennas

arrival of the spoofing signals remains constant. Therefore, the AOA can be determined by measuring the different phases of the same spoofing signal arriving at different antennas in a uniform linear array. [125, 126] were the first to achieve sub-meter localization accuracy, reaching 0.7 m. Subsequently, University College London leveraged multiple-input multiple-output (MIMO) technology and channel state information (CSI) to measure AOA, achieving a remarkable localization accuracy of 23 cm [127].

The accuracy of the two-step localization method is highly dependent on the accuracy of the parameter estimation. The location calculation and parameter estimation are inseparable, limiting the effective utilization of correlations between signals received at different stations, leading to information loss, difficulties correlating localization parameters, and high system sensitivity requirements. Clock offset, however, contains information about the location of the spoofing interference source relative to the receiver. Utilizing the clock offset measured at different receiver locations under both genuine and spoofing interference signal conditions allows for calculating the distance difference between the spoofing interference source and the two receivers. The location of the spoofing interference source can be estimated using hyperbolic intersection localization by employing multiple sets of receivers to measure these distance differences.

4.4 Summary

This article summarizes the scenarios to which the commonly used anti-spoofing methods of various receivers are applicable, what kind of spoofing signal characteristics apply, and what functions the receiver needs to have, as shown in Table 4 below.

5 Opportunities and challenges

As satellite navigation systems continue to evolve, dependence on these systems will inevitably increase, making the threat of satellite navigation spoofing interference increasingly prominent. Consequently, intensifying research and preventative measures, along with developing more intelligent and advanced anti-interference technologies, are crucial. Several challenges persist in the field of anti-spoofing interference:

First, the quality of spoofed signals continues to improve, resulting in enhanced concealment, increased positional and velocity accuracy, higher generation frequencies, and a closer resemblance to genuine signals. This allows spoofed signals to seamlessly and covertly integrate into receivers, posing significant challenges for anti-spoofing measures. Second, the maturation of multi-spoofing interference platform technologies has introduced a paradigm shift from single-platform spoofed signals. These multi-platform systems generate interference signals from multiple directions and utilize diverse interference types simultaneously, demanding higher anti-interference capabilities from receivers. Third, current experimental conditions for spoofing interference are overly idealized, primarily conducted in open, sparsely populated areas with minimal radio signal interference. Limited research has been conducted in complex terrain, such as mountainous regions and urban areas. The lack of experimental materials for such scenarios significantly hinders the development of effective anti-spoofing interference technologies. Meanwhile, spoofing techniques are constantly evolving. Attack methods such as security code estimation and replay (SCER), which differ from traditional spoofing methods, are becoming increasingly cost-effective [128]. With multiple spoofing methods working in

tandem, receivers face a significant challenge in handling scenarios where multiple spoofing attacks coexist.

To address these challenges, future satellite navigation receivers must adopt a combined approach to anti-interference detection. This approach should leverage machine learning, consistency checks, and array testing to enable more effective and robust spoofing interference detection [129]. Additionally, by combining the performance advantages of multiple research projects, a multi-faceted aerial defense system could be developed using unmanned aerial vehicle (UAV) clusters, ships, and aircraft. This system would encompass target identification and tracking, radio countermeasures, and multi-target strikes. Finally, compact anti-interference platforms should be developed to enhance the stability of anti-spoofing measures by making anti-interference receivers portable, miniaturized, and cost-effective.

Author contributions

CL: Writing–review and editing. ZLu: Supervision, Resources, Project administration, writing–review and editing. Zli: Supervision, Resources, Writing–review and editing. LH: Supervision, Resources, Writing–review and editing. FC: Supervision, Resources, Writing–review and editing.

Funding

The author(s) declare that financial support was received for the research, authorship, and/or publication of this article from the National Natural Science Foundation of China under Grant U20A0193.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

1. Margaria D, Motella B, Anghileri M, Floch J-J, Fernández-Hernández I, Paonni M. Signal structure-based authentication for civil GNSSs: recent solutions and perspectives. *IEEE Signal Process. Mag* (2017) 34(5):27–37. doi:10.1109/msp.2017.2715898

2. Kaplan ED. GPS principles and applications. In: *Translated by kou yan-hong*. 2nd ed. Beijing: Electronic Industry Press (2007).

3. Chen Y, Zhan X.GNSS vulnerability reliable assessment and its substitution with visual-inertial navigation[J]. *Aerospace Syst*, 2021, Vol.4(3): 179–89. doi:10.1007/s42401-021-00099-6

4. Jovanovic A, Botteron C, Fariné P-A. Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers. In: *Proc. IEEE/ION position, location navigat. Symp. (PLANS)*. Monterey, CA, USA (2014).12581271

5. Psiaki ML, Humphreys TE, Stauffer B. Attackers can spoof navigation signals without our knowledge. Here's how to get back GPS lies. *IEEE Spectr* (2016) 53(8): 26–53. doi:10.1109/MSPEC.2016.7524168

6. Heng L, Work DB, Gao GX. GPS signal authentication from cooperative peers. *IEEE Trans Intell Transp Syst* (2015) 16(4):1794–805. doi:10.1109/tits.2014.2372000

7. Jiang C, Chen S, Chen Y, Bo Y, Xia Q, Zhang B. Analysis of the baseline data based GPS spoofing detection algorithm. In: *Proc. IEEE/ION position, location navigat*. Monterey, CA, USA (2018). Symp. (PLANS).397403

8. Xie X, Lu M, Zeng D. Research on GNSS generating spoofing jamming technology. In: *Proc. IET int. Radar conf*. Hangzhou, China (2015). p. 5. doi:10.1049/cp.2015.0999

9. He L, Li W, Guo C, Niu R. Civilian unmanned aerial vehicle vulnerability to GPS spoofing attacks. In: *2014 seventh international symposium on computational intelligence and design*. Hangzhou, China (2014). p. 212–5. doi:10.1109/ISCID.2014.131

10. Kugler LOGAN. Why GPS spoofing is a threat to companies, countries. *Commun ACM* (2017) 60(9):18–9. doi:10.1145/3121436

11. Jon S, Warner PD, Roger P, Johnston G. "GPS spoofing countermeasures." (2003).

12. Humphreys TE, Ledvina BM, Psiaki ML, O'Hanlon BW, Kintner PM, Jr. Assessing the spoofing threat: development of a portable GPS civilian spoofer. In: *Proceedings of the 21st international technical meeting of the satellite division of the Institute of navigation (ION GNSS 2008)*. Savannah, GA (2008). p. 2314–25.

13. Hu Y, Bian S, Li B, Zhou L. A novel array-based spoo ng and jamming suppression method for GNSS receiver. *IEEE Sensors J* (2018) 18(7):2952–2958. doi:10.1109/JSEN.2018.2797309

14. Zhang N. A case study on the application of GPS forward spoofing jamming in UAV. *Aerosp China* (2015) 7:4042.

15. Shepard DP, Bhatti JA, Humphreys TE, Fansler AA. "Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks," in Proceedings of the 25th international technical meeting of the satellite division of The Institute of Navigation (ION GNSS 2012), Nashville, TN (2012). 3591–3605.

16. Humphreys TE. UT austin researchers spoof supery acht at sea (2013). Austin: The University of Texas at Austin. Available from: http://www.engr.utexas.edu/features/superyacht-gps-spoofng.

17. Psiaki ML, Humphreys TE. GNSS spoofing and detection. *Proc IEEE* (2016) 104(6):1258–70. doi:10.1109/JPROC.2016.2526658

18. Bian S, Hu Y, Ji B. Research status and prospect of GNSS anti-spoofing technology. *Scientia Sinica Informationis* (2017) 47(3):275–287. doi:10.1360/N112016-00073

19. Dai SG, Zhou HJ. GNSS repeater detection based on channel difference. *J Comput Methods Sci Eng* (2018) 18(2):491–8. doi:10.3233/jcm-180804

20. Bian SF, Hu YF, Chen C, Li ZM, Ji B, et al. Research on GNSS repeater spoofing technique for fake position, fake time and fake velocity [C]. In: *IEEE international conference on advanced intelligent mechatronics* (Munich, Germany: AIM) (2017). p. 1430–1434. doi:10.1109/AIM.2017.8014219

21. Jun WANG, Yan GUO, Tang K, He X. Navigation and control,2022, Vol.21(1): 13–24.

22. He T. Improvement of GNSS transponder deception jamming method. *Bull Surv Mapp* (2019) 0 (4) 71–74,83. doi:10.13474/j.cnki.11-2246.2019.0115

23. Farley MG, Carlson SG. "A new pseudolite battlefield navigation system," in *IEEE 1998 Position Location and Navigation Symposium (Cat. No.98CH36153)* (Palm Springs, CA, United States) (1998):208–217. doi:10.1109/PLANS.1998.670043

24. Zhang S, Yang J, Gaofeng P, Jiabao J. GPS area-mapping deceiving unites region navigation integrative system. In: *2010 3rd international conference on computer science and information technology*. Chengdu (2010). p. 189–91. doi:10.1109/ICCSIT.2010.5564940

25. Jafarnia-Jahromi A, Broumandan A, Nielsen J, Lachapelle G. GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements. *Int J Satellite Commun Networking* (2012) 30(4):181–91. doi:10.1002/sat.1012

26. Humphreys TE, Brent ML, Mark LP, Brady WO'H, Paul MK. Assessing the spoofing threat: development of a portable GPS civilian spoofer. In: *Proceedings of the ION GNSS meeting* (2008). p. 16–9.

27. Gao Y, Lv Z, Zhang L. Asynchronous lift-off spoofing on satellite navigation receivers in the signal tracking stage. *IEEE Sens J* (2020) 20(15):8604–13. doi:10.1109/jsen.2020.2984525

28. Wang J, Zhou M, Li H, Cui X, Lu M. "On the requirements of GNSS intermediate spoofing," in China satellite navigation conference (CSNC) 2014 proceedings: volume I, New Delhi, India. Editor Sun J., Jiao W., Wu H., Lu M. (Springer, Berlin, Heidelberg:

Lecture Notes in Electrical Engineering) (2014) 303. doi:10.1007/978-3-642-54737-9_47

29. Geng Z. *Research on GNSS spoofing jamming detection and suppression technology*. Ph.D. Dissertation, National University of Defense Technology (2019). doi:10.27052/d.cnki.gzjgu.2019.000344

30. Ioannides RT, Pany T, Gibbons G. Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques. *Proc IEEE* (2016) 104(6): 1174–94. doi:10.1109/jproc.2016.2535898

31. Gang X. *GPS principle and receiver design[M]*. Electronics Industry Press (2017).

32. Yang Q. *Research on anti-jamming technology of satellite navigation receiver[D]*. Northwestern Polytechnical University (2019).

33. Fan G, Huang Y, Zhang G, Nie J, The GPS spoofing detection based on the joint WSSE of DOA and pseudorange[C].

34. Akos DM. Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). *J Navigation* (2012) 59(4):281–90. doi:10.1002/navi.19

35. Dehghanian V, Nielsen J, Lachapelle G. GNSS spoofing detection based on signal power measurements: statistical analysis. *Int J Navigation and Observation* (2012) 2012(7):1–8. doi:10.1155/2012/313527

36. Dehghanian V, Nielsen J, Lachapelle G. GNSS spoofing detection based on receiver C/N0 estimates[J]. *Proceedings of international technical meeting of the satellite division of the Institute of navigation*, 2012:2878–84.

37. Nielsen J, Dehghanian V, Lachapelle G. Effectiveness of GNSS spoofing countermeasure based on receiver CNR measurements. *Int J Navig Observations* (2012) 2012(9):1–9. doi:10.1155/2012/501679

38. Long H, Tang X, Feixue W. Research on anti-spoofing jamming method of satellite navigation receiver[C]. In: *China satellite navigation academic annual conference* (2011). p. 1344–7.

39. Gao Y, Li H, Lu M, Feng Z. Intermediate spoofing strategies and countermeasures [J], *Tsinghua Science and Technology*, 2013.18(6), 599–605. doi:10.1109/TST.2013.6678905

40. Tu JX, Zhan XQ, Zhang X, Zhang ZJ, Jing S. Low-complexity GNSS anti-spoofing technique based on Doppler frequency difference monitoring. *IET Radar, Sonar and Navigation* (2018) 12(9):1058–65. doi:10.1049/iet-rsn.2018.5151

41. Wullems CJ. A spoofing detection method for civilian L1 GPS and the E1-B galileo safety of life service. *IEEE Trans Aerospace Electron Syst* (2012) 48(4):2849–64. doi:10.1109/taes.2012.6324665

42. Motella B, Pini M, Fantino M, Mulassano P, Nicola M, Fortuny Guasch J, et al. Performance assessment of low cost GPS receivers under civilian spoofing attacks[C]. Noordwijk, Netherlands: 2010 5th ESA Workshop on satellite navigation technologies and European workshop on GNSS signals and signal processing (NAVITEC) (2010) 1–8. doi:10.1109/NAVITEC.2010.5708018

43. Psiaki ML, Ohanlon BW, Powell SP, Bhatti JA, Wesson KD, Schofield TE. Humphreys andrew, GNSS spoofing detection using two-antenna differential carrier phase. In: *Proceedings of the 27th international technical meeting of the satellite division of the Institute of navigation (ION GNSS+ 2014)*. Florida: Tampa (2014). p. 2776–800.

44. Savasta S, Presti LL, Dovis F, Margaria D. Trustworthiness GNSS signal validation by a time-frequency approach[C]. In: *Proceedings of the 22nd international technical meeting of the satellite division of the Institute of navigation (ION GNSS 2009)* (2009). p. 66–75.

45. Jafarnia-Jahromi A, Lin T, Broumandan A, Nielsen J, Lachapelle G. Detection and mitigation of spoofing attacks on a vector based tracking GPS receiver[C]. In: *Proceedings of international technical meeting of the Institute of navigation (ION ITM 2012)*. Newport Beach, CA. p. 790–800. 30 January-1 February.

46. Cavaleri A, Motella B, Pini M, Fantino M. *Detection of spoofed GPS signals at code and carrier tracking level*. Noordwijk, Netherlands: 2010 5th ESA Workshop on satellite navigation technologies and European workshop on GNSS signals and signal processing (NAVITEC) (2010). p. 1–6. doi:10.1109/NAVITEC.2010.5708016

47. Broumandan A, Jafarnia-Jahromi A, Dehghanian V, Nielsen J, Lachapelle G. GNSS spoofing detection in handheld receivers based on signal spatial correlation[C]. In: *Proceedings of IEEE/ION PLANS 2012*. p. 479–87. April 24-26, Myrtle Beach, South Carolina.

48. Shen C, Guo C. Simulation of optimal detection of spoofing signals in global navigation satellite system[J]. *Computer Simulation*, 2019, 36(6):109–113, 119. doi:10.3969/j.issn.1006-9348.2019.06.022

49. He H. Research on anti-spoofing jamming method of satellite navigation based on array[D]. In: *Heilongjiang*. Harbin Engineering University, MA thesis (2019).

50. Rui X, Mengyu D, Qian M. MEDLL-assisted spoofing signal identification method for GNSS/INS system[J]. *Chin J Inertial Technology*, 2018, v.26(02):89–96. doi:10.13695/j.cnki.12-1222/o3.2018.02.013

51. Yin W, Yang GG, Fu J. Interference identification for inertial assisted GNSS receivers[J]. *J Navigation Positioning*, 2018, v.6;No. 22(02):45–49. doi:10.16547/j.cnki.10-1096.20180208

52. Yabin L, Guo C, Zhong T. Research on GPS anti-spoofing jamming based on zeroing technology. *Electro-Optics and Control*, 2017(01):41–44. doi:10.3969/j.issn.1671-637X.2017.01.009

53. Liu D, Lv J, Rui M, et al. Research and prospect of spoofing and anti-spoofing technology of satellite navigation system[J]. *Res Beidou Satellite Navigation Signal Spoofing Jamming Detect Technology*, 2017, 50(05):837–843. doi:10.3969/j.issn.1002-0802.2017.05.001

54. Cao K, Peng X, Bao LI, et al. Spoofing jamming detection method based on signal-to-noise ratio measurement[J]. *Computer Meas and Control*, 2016, 24(04):29–32+35. doi:10.16526/j.cnki.11-4762/tp.2016.04.009

55. Wesson KD, Gross JN, Humphreys TE, Evans BL. GNSS signal authentication via power and distortion monitoring. *IEEE Trans Aerospace Electron Syst* (2018) 54(2): 739–54. doi:10.1109/TAES.2017.2765258

56. Shuli D, Taotao Z, Min L. A GNSS anti-spoofing technology based on power detection. In: *2019 IEEE 8th joint international information technology and artificial intelligence conference (ITAIC)*. Chongqing, China (2019). p. 1134–7. doi:10.1109/ITAIC.2019.8785690

57. Zhang G, Zhang Y, Ye TIAN. Research on Beidou deceptive jamming detection technology based on DOD and PTD. *Appl Sci Technology* (2019) 46(2):35–41. doi:10.11991/yykj.201807010

58. Fan G, Ran D, Zhang F, Zhouhui TUO.*Glob Positioning Syst*, 2020, 45(1):66–70. doi:10.13442/j.gnss.1008-9268.2020.01.011

59. Wang Z, Nie J, Zhengrong L. Forwarded spoofing signal detection algorithm for BOC receiver capture stage [J]. *Glob Positioning Syst*, 2016, 41(05):13–17. doi:10.13442/j.gnss.1008-9268.2016.05.003

60. Zhang G, Ding J, Zhang Y. Relay spoofing jamming detection algorithm based on GNSS signal delay feature [J]. *Radio Eng*, 2019, 49(07):626–630. doi:10.3969/j.issn.1003-3106.2019.07.015

61. Wang W, Wang P. GNSS spoofing jamming detection based on capture results [J]. *J Signal Process*, 2021, 37(08):1460–1469. doi:10.16798/j.issn.1003-0530.2021.08.013

62. Jian W, Hong L, Cui X, et al. "A new method in acquisition to detect GNSS spoofing signal [C]," in Proceedings 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer, Shenyang, China (2014). p. 2913–2917.

63. Yang B, Mei T, Ji Y, Cheng J, Xie Z, Shao S. Research on GNSS spoofing mitigation technology based on spoofing correlation peak cancellation. *IEEE Commun Lett* (2022) 3024–8. doi:10.1109/LCOMM.2022.3204944

64. Daneshmand S, Jafarnia-Jahromi A, Broumandan A. A GNSS structural interference mitigation technique using antenna array processing [C]. *IEEE 8th sensor array multichannel signal process workshop*, Coruna, Spain, 2014: 109–12.

65. Da-Jiang GE, Zhou GB, Da-Chuan XU. GPS receiver anti-deceptive jamming method based on space-time multi-antenna null [J]. *J Sichuan Ordnance*, 2015, 36(8): 41–45.

66. Long H, Ling Y, Bo X, et al. Anti-spoofing method for satellite navigation receiver using dual-antenna carrier phase difference technology[J]. *J Natl Univ Defense Technology*, 2016, 38(04): 103–106. doi:10.11887/j.cn.201604016

67. Hu Y, Bian S, Li B, Zhou L. A novel array-based spoofing and jamming suppression method for GNSS receiver. *IEEE Sensors J* (2018) 18(7):2952–8. doi:10.1109/jsen.2018.2797309

68. Jiang C, Chen S, Chen Y. Analysis of the baseline data based GPS spoofing detection algorithm [C]//IEEE/ION Position. In: *Location and navigation symposium*. Monterey, USA (2018). p. 397–403.

69. Wang F, Li H, Lu M. GNSS spoofing detection based on unsynchronized double-antenna measurements. *IEEE Access* (2018) 6:31203–12. doi:10.1109/access.2018.2845365

70. Nguyen VH, Falco G, Nicola M, Falletti E. *A dual antenna GNSS spoofing detector based on the dispersion of double difference measurements [C]//2018 9th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing*. Noordwijk, Netherlands: 2018 9th ESA workshop on satellite navigation technologies and European workshop on GNSS signals and signal processing (NAVITEC) (2018). p. 1–8. doi:10.1109/NAVITEC.2018.8642705

71. Xu G, Shen F, Amin M, Wang C. DOA classification and CCPM-PC based GNSS spoofing detection technique [C]. In: *2018 IEEE/ION position, location and navigation symposium (PLANS)*. Monterey, CA, USA (2018). p. 389–396. doi:10.1109/PLANS.2018.8373405

72. van der Merwe JR, Rügamer A, Goicoechea AFD, Felber W. "Blind spoofing detection using a multi-antenna snapshot receiver," in *2019 international conference on localization and GNSS (ICL-GNSS)*. Nuremberg, Germany (2019). p. 1–7. doi:10.1109/ICL-GNSS.2019.8752840

73. Xiao L, Li X, Wang G. GNSS spoofing detection using pseudo-range double differences between two receivers [C]. In: *2019 IEEE 7th international conference on computer science and network technology*. Dalian, China (2019). p. 498–502.

74. Xiao L, Li X, Liao Z. GNSS spoofing detection with using linear array [C]. In: *2020 IEEE 8th international conference on computer science and network technology*. Dalian, China (2020). p. 181–5.

75. Mingfeng Q, Lige H, Kexin L. A deception interference detection method based on multi-baseline carrier phase difference measurement[J]. *Navigation, Positioning and Timing*, 2021, 8(03): 68–74. doi:10.19306/j.cnki.2095-8110.2021.03.009

76. Wang X, Wu S, Wang Y, et al. A method for detecting and suppressing spoofing jamming in satellite navigation based on array antenna[J]. *Mod Navigation*, 2022, 13(03):163–169. doi:10.3969/j.issn.1674-7976.2022.03.002

77. Yang H, Jin R, Xu W, Che L, Weimin Z. Satellite navigation spoofing interference detection and direction finding based on array antenna. *Sensors* (2023) 23(3):1604. doi:10.3390/s23031604

78. Jovanovic A, Botteron C, Fariné PA. Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers [C]//IEEE/ION Position. In: *Location and navigation symposium*. Monterey, CA, USA (2014). p. 1258–71.

79. Tu J, Zhan X, Zhang X, Zhang Z, Jing S. Low-complexity GNSS anti-spoofing technique based on Doppler frequency difference monitoring. *IET Radar, Sonar and Navigation* (2018) 12(9):1058–65. doi:10.1049/iet-rsn.2018.5151

80. Tu J, Zhan X, Chen M, Gao H, Chen Y. GNSS intermediate spoofing detection via dual-peak infrequency domain and relative velocity residuals. *IET Radar, Sonar and Navigation* (2020) 14(3):439–47. doi:10.1049/iet-rsn.2019.0366

81. Li H, Hong L, Mingquan L. Global navigation satellite system spoofing-detection technique based on the Doppler ripple caused by vertical reciprocating motion. *Radar, Sonar and Navigation, IET* (2019) 13(10):1655–64. doi:10.1049/iet-rsn.2019.0058

82. Yuan D, Li H, Wang F, Lu M. A GNSS acquisition method with the capability of spoofing detection and mitigation, 27. *Chin J of Electronics* (2018). p. 213–22. doi:10.1049/cje.2017.11.001

83. Chu F, Li H, Wen J, Lu M. Statistical model and performance evaluation of a GNSS spoofing detection method based on the consistency of Doppler and pseudorange positioning results. *J Navigation* (2019) 72(2):447–66. doi:10.1017/S0373463318000747

84. Zhang G, Zhang Y, Tian Y. Research of Beidou navigation satellite system (BDS) spoofing detection based on DOD and PTD. *Appl Sci Technol* (2019) 46(2):3541. doi:10.11991/yykj.201807010

85. Li J, Zhu X, Ouyang M, Shen D, Chen Z, Dai Z. GNSS spoofing detection technology based on Doppler frequency shift difference correlation. *Meas Sci Technol* (2022) 33:095109. doi:10.1088/1361-6501/ac672a

86. Wei X, Sun C, Li X, Ma J. GNSS spoofing detection for UAVs using Doppler frequency and Carrier-to-Noise Density Ratio. *J Syst Archit* (2024) 153:103212. doi:10.1016/j.sysarc.2024.103212

87. Phelts R, Eric. *Multicorrelator techniques for robust mitigation of threats to GPS signal quality[D]*. California: Stanford University (2001).

88. Wang W, Li N, Wu R, Closas P. Detection of induced GNSS spoofing using S-curve-bias. *Sensors(Basel Switzerland)* (2019) 19(4):922. doi:10.3390/s19040922

89. Sun C, Cheong JW, Dempster AG, Zhao H, Feng W. GNSS spoofing detection by means of signal quality monitoring(SQM)metric combinations. *IEEE Access* (2018) 6: 66428–41. doi:10.1109/access.2018.2875948

90. Pirsiavash A, Broumandan A, Lachapelle G. Two-dimensional signal quality monitoring for spoofing detection. *NAVITEC* (2016).

91. Sun C, Cheong JW, Dempster AG, Demicheli L, Cetin E, Zhao H, et al. Moving variance-based signal quality monitoring method for spoofing detection. *GPS Solut* (2018) 22:83. doi:10.1007/s10291-018-0745-7

92. Wang W, Gong J, Wang J. GNSS spoofing jamming detection algorithm based on SCB variance[J]. *Syst Eng Electronics*, 2021, 43(8):2254–2262. doi:10.12305/j.issn.1001-506X.2021.08.27

93. Zhou W, Lv Z, Deng X, Ke Y. A new induced GNSS spoofing detection method based on weighted second-order central moment. *IEEE Sensors J* (2022) 22(12): 12064–78. doi:10.1109/JSEN.2022.3174019

94. Benachenhou K, Bencheikh ML. Detection of global positioning system spoofing using fusion of signal quality monitoring metrics. *Comput Electr Eng* (2021) 92:107159. doi:10.1016/j.compeleceng.2021.107159

95. Miralles D, Bornot A, Rouquette P, Levigne N, Akos DM, Chen YH, et al. An assessment of GPS spoofing detection via radio power and signal quality monitoring for aviation safety operations. *IEEE Intell Transportation Syst Mag* (2020) 12(3):136–46. Fall. doi:10.1109/MITS.2020.2994117

96. Sun C, Cheong JW, Dempster AG, Zhao H, Bai L, Feng W. Robust spoofing detection for GNSS instrumentation using Q-channel signal quality monitoring metric. *IEEE Trans Instrumentation Meas* (2021) 70:1–15. Art no. 8504115. doi:10.1109/TIM.2021.3102753

97. Blum R, Pany T. *Spoofing defense concept based on the combination of SQM and tracking parameters, tested against 100 simulated spoofer settings for GPS L1 C/A*. The International Technical Meeting of the The Institute of Navigation (2022). n. pag. doi:10.33012/2022.18184

98. Zhang X, Li H, Yang C, Lu M. Signal quality monitoring-based spoofing detection method for Global Navigation Satellite System vector tracking structure. *IET Radar, Sonar and Navigation* (2020) 14:944–53. doi:10.1049/iet-rsn.2020.0021

99. Zhou W, Lv Z, Li G, Jiao B, Wu W. Detection of spoofing attacks on global navigation satellite systems using Kolmogorov–smirnov test-based signal quality monitoring method. *IEEE Sensors J* (2024) 24(7):10474–90. doi:10.1109/JSEN.2024.3354110

100. Shen J. *Research on jamming recognition technology in communication countermeasures[D]*. University of Electronic Science and Technology of China, MA thesis (2011). p. 7–9.

101. Cohen WW, Richman J. Learning to match and cluster large high-dimensional data sets for data integration[C]. In: *Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining* (2002). p. 475–80.

102. Yu Y, Zhong-liang F, Xiang-hui Z, Wen-fang C. *Combining Classifier Based on Decision Tree*. Taiyuan, China: 2009 WASE International Conference on Information Engineering (2009) 2:37–40. doi:10.1109/ICIE.2009.12

103. Yue L. *Research on communication interference pattern recognition and parameter estimation algorithm[D]*. Xidian University, MA thesis (2019). p. 31–3. doi:10.27389/d.cnki.gxadu.2019.001061

104. Xun L, Lu N, Qiang W Communication signal modulation mechanism recognition technology based on BP neural network[J]. *Telecommunications Technology*, 2006, 46(1):143–146. doi:10.3969/j.issn.1001-893X.2006.01.031

105. Ruoran F. Compound jamming signal recognition based on neural networks[C]. In: *Sixth international conference on instrumentation and measurement*. IEEE (2016). p. 737–40.

106. Jiang M. *Identification and localization of multiple interference sources for satellite navigation[D]*. Xi'an University of Technology, MA thesis (2020) doi:10.27398/d.cnki.gxalu.2020.000518

107. Wu Y. Research on classification algorithm based on decision tree[J]. *Digital Commun World*, 2017, No. 156(12):268–269). doi:10.3969/J.ISSN.1672-7274.2017.12.232

108. Zhu L. *Research and implementation of interference identification and direction finding technology of Beidou satellite navigation satellite system[D]*. Beijing Jiaotong University, MA thesis (2019). p. 35–57. doi:10.26944/d.cnki.gbfju.2019.000581

109. Dang Z. *Research on wireless communication interference signal recognition and processing technology based on deep learning[D]*. University of Electronic Science and Technology of China, MA thesis (2020). p. 13–38. doi:10.27005/d.cnki.gdzku.2020.004101

110. Kong M, Liu J, Zhang Z, Qiao Y. Radio ground-to-air interference signals recognition based on support vector machine[C]. Singapore: 2015 IEEE International Conference on Digital Signal Processing (DSP) (2015). p. 987–990. doi:10.1109/ICDSP.2015.7252025

111. Wang G -S, Ren Q -H, Su Y -Z. The interference classification and recognition based on SF-SVM algorithm. In: *2017 IEEE 9th international conference on communication software and networks (ICCSN)*. Guangzhou, China (2017). p. 835–41. doi:10.1109/ICCSN.2017.8230229

112. Iqbal A, Aman MN, Sikdar B, "A deep learning based induced GNSS spoof detection framework," in *IEEE transactions on machine learning in communications and networking*, vol. 2, pp. 457–78. 2024. doi:10.1109/TMLCN.2024.3386649

113. Liu Y, Li S, Fu Q, Liu Z, Zhou Q. Analysis of Kalman filter innovation-based GNSS spoofing detection method for INS/GNSS integrated navigation system. *IEEE Sensors J* (2019) 19(13):5167–78. doi:10.1109/jsen.2019.2902178

114. Zhang C, Lyv Z, Zhang L. A spoofing detection algorithm for INS/GNSS integrated navigation system based on innovation rate and robust estimation [J]. *J Chin Inertial Technology*, 2021, 29(3): 328–333. doi:10.13695/j.cnki.12-1222/o3.2021.03.008

115. Ceccato M, Formaggio F, Laurenti N, Tomasin S. Generalized likelihood ratio test for GNSS spoofing detection in devices with IMU. *IEEE Trans Inf Forensics Security* (2021) 16:3496–509. doi:10.1109/tifs.2021.3083414

116. Clements Z, Yoder J E, Humphreys T. Carrier-phase and IMU based GNSS spoofing detection for ground vehicles. In: *Proceedings of the 2022 international technical meeting of the Institute of navigation*. Long Beach, California, USA (2022). p. 83–95.

117. Cui J, Cheng N, Ni S. Research on suppression method of spoofed navigation jamming signal by array antenna [J]. *Acta Electronica Sinica*, 2018, 46(2):365–71. doi:10.3969/j.issn.0372-2112.2018.02.015

118. Guo Y, Fan M, Kong M. Spoofing interference suppression using space-time process for GNSS receiver. *Int Congress Image Signal Process* (2012) 1537–1541. doi:10.3969/j.issn.1003-0530.2007.04.018

119. Broumandan A, Jafarnia-Jahromi A, Lachapelle G. Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver. *GPS Solut* (2015) 19:475–87. doi:10.1007/s10291-014-0407-3

120. Sun X, Wu Z, Nie Y. A new satellite navigation spoofing jamming suppression method. In: *Proceedings of the 9th China satellite navigation academic annual conference S03 satellite navigation signal and anti-jamming technology* (2018). p. 28–32.

121. Zhang J, Gui L, Yuan Y, et al. Array anti-spoofing method based on GNSS multi-channel tracking receiver[J]. *Telecommunication Technology*, 2023, 63(6):817–825). doi:10.20079/j.issn.1001-893x.230106004

122. Hans S, Chen L, Meng W, Li C, et al. Improve the security of GNSS receivers through spoofing mitigation[J]. *IEEE Access*, 2017, 5:21057–21069. doi:10.1109/ACCESS.2017.2754414

123. Zhao H, Lian B, Feng J. ADAPTIVE BEAMFORMING ALGORITHM FOR INTERFERENCE SUPPRESSION IN GNSS RECEIVERS. *Int J Computer Sci Inf Technology* (2011) 3:17–28. doi:10.5121/ijcsit.2011.3502

124. Shang X, Sun F, Zhang L, Cui J, Zhang Y. Detection and mitigation of GNSS spoofing via the pseudorange difference between epochs in a multicorrelator receiver. *GPS Solut* (2022) 26:37. doi:10.1007/s10291-022-01224-4

125. Kotaru M, Joshi KR, Bharadia D, Katti S. SpotFi: decimeter level localization using WiFi. In: *Proceedings of the 2015 ACM conference on special interest group on data communication* (2015). n. pag.

126. Tian Z, Li Z, Zhou M, Jin Y, Wu Z. PILA: sub-meter localization using CSI from commodity wi-fi devices. *Sensors* (2016) 16(10):1664. doi:10.3390/s16101664

127. Sen S, Radunovic B, Choudhury RR, Minka T. You are facing the Mona Lisa: spot localization using PHY layer information. In: *Proceedings of the 10th international conference on Mobile systems, applications, and services (MobiSys,12)*. New York, NY, USA: Association for Computing Machinery (2012). p. 183–96. doi:10.1145/2307636.2307654

128. Li X, Lu Z, Yuan M, Liu W, Wang F, Yu Y, et al. Tradeoff of code estimation error rate and terminal gain in SCER attack. *IEEE Trans Instrumentation Meas* (2024) 73:1–12. doi:10.1109/tim.2024.3406807

129. Zhang X. A review of satellite navigation spoofing jamming signal detection technology. *Glob Positioning Syst* (2018) 43(6):1–7. doi:10.13442/j.gnss.1008-9268.2018.06.001