sensors

MDPI

Review

Detecting and Mitigating Attacks on GPS Devices

Jack Burbank *, Trevor Greene and Naima Kaabouch *

Artificial Intelligence Research (AIR) Center, University of North Dakota, Grand Forks, ND 58202, USA; trevor.greene@und.edu

* Correspondence: jack.burbank@und.edu (J.B.); naima.kaabouch@und.edu (N.K.)

Abstract: Modern systems and devices, including unmanned aerial systems (UASs), autonomous vehicles, and other unmanned and autonomous systems, commonly rely on the Global Positioning System (GPS) for positioning, navigation, and timing (PNT). Cellular mobile devices rely on GPS for PNT and location-based services. Many of these systems cannot function correctly without GPS; however, GPS signals are susceptible to a wide variety of signal-related disruptions and cyberattacks. GPS threat detection and mitigation have received significant attention recently. There are many surveys and systematic reviews in the literature related to GPS security; however, many existing reviews only briefly discuss GPS security within a larger discussion of cybersecurity. Other reviews focus on niche topics related to GPS security. There are no existing comprehensive reviews of GPS security issues in the literature. This paper fills that gap by providing a comprehensive treatment of GPS security, with an emphasis on UAS applications. This paper provides an overview of the threats to GPS and the state-of-the-art techniques for attack detection and countermeasures. Detection and mitigation approaches are categorized, and the strengths and weaknesses of existing approaches are identified. This paper also provides a comprehensive overview of the state-of-the-art on alternative positioning and navigation techniques in GPS-disrupted environments, discussing the strengths and weaknesses of existing approaches. Finally, this paper identifies gaps in existing research and future research directions.

Keywords: global positioning system; GPS security; GPS jamming; GPS spoofing; GPS-denied; environments

check for updates

Citation: Burbank, J.; Greene, T.; Kaabouch, N. Detecting and Mitigating Attacks on GPS Devices. *Sensors* **2024**, *24*, 5529. https://doi.org/10.3390/s24175529

Academic Editor: Habib Ammari

Received: 9 June 2024
Revised: 8 August 2024
Accepted: 16 August 2024
Published: 26 August 2024

1. Introduction

Modern systems and devices commonly rely on the Global Positioning System (GPS) for positioning, navigation, and timing (PNT). Manned and unmanned airplanes, ships, and ground vehicles typically rely on GPS for positioning and navigation. Unmanned autonomous systems, such as unmanned aerial systems (UASs), rely on GPS to support navigation. Cellular mobile devices utilize these navigation signals for self-positioning and supporting location-based services and applications.

Reliable and accurate positioning and navigation are paramount for safe and reliable UAS operations. A UAS must typically maintain an accurate record of where it has been, where it currently is, and where it is going to successfully complete its task. An unmanned sensor often needs to know its location for its measurements to be useful. A UAS must be capable of conducting accurate navigation to maintain flight safety. Autonomous unmanned operations are not possible without reliable positioning and navigation capabilities. A common approach to providing reliable UAS positioning and navigation is through the use of a Global Navigation Satellite System (GNSS), such as a GPS, which provides a series of signals from space-based satellites that ground or air-based systems use to determine their location and typically serves as a primary input into the system's guidance and navigation system. These receivers are now integrated into billions of manned and unmanned commercial and military devices; however, GPS signals are susceptible to a wide variety of factors and may not always be available or trustworthy. Positioning accuracy can be significantly degraded in complex propagation environments that induce multipath fading or signal shadowing effects. These navigation signals can also be degraded or completely disrupted by intentional or unintentional interference. For example, GPS signals are vulnerable to intentional jamming and spoofing attacks, which can lead to a loss of positioning and navigation integrity. These issues can lead to significant vulnerabilities in commercial and military infrastructure and the degradation or malfunction of vehicles and systems, such as UASs.

The loss of GPS signal integrity is a serious issue for manned and unmanned systems; however, it is particularly problematic for unmanned systems. A human operator can use other means for navigation if GPS-based positioning is unavailable in a manned system, including the use of on-hand information such as maps, landmark recognition such as street signs, the use of other navigation devices such as a magnetic compass, or collaboration with others, such as asking others for their current location. Human operators also have the cognitive means to fuse these alternate data sources to provide a reliable position estimation. Unmanned systems may have access to additional data sources, other sensors, and perhaps even collaboration opportunities with other manned or unmanned systems; however, they must possess the intelligence to process and fuse this information to estimate position autonomously. Furthermore, unmanned systems come in various form factors and cost points, which may limit the types of onboard sensing or processing available for positioning and navigation.

Many studies reported in the literature have attempted to characterize the performance of GPS positioning in complex propagation environments and proposed methods to augment GPS-based positioning with other sensor types that may be onboard a system, such as visual methods using an onboard camera. Numerous approaches have been proposed to provide autonomous methods to detect or mitigate the effects of hostile jamming and spoofing. Furthermore, many non-GNSS methods of positioning and navigation in GPS-denied environments exist. Many surveys and systematic reviews on GPS security and alternate positioning and navigation methods have been published; however, many only briefly discuss GPS security within a larger cybersecurity discussion. Other reviews focus on niche topics related to GPS security or alternative non-GNSS positioning and navigation methods. There are no existing comprehensive reviews of GPS security issues in the literature. This paper fills that gap by providing a comprehensive treatment of GPS security.

We provide an overview of the factors that can degrade or disrupt GPS signals in this paper, particularly those related to cybersecurity. Section 2 summarizes previous surveys and systematic reviews related to GPS security. Section 3 introduces GPS and establishes the performance baselines of GPS systems in benign conditions. Section 4 discusses the various disruption scenarios, attack types, and threat systems that can affect successful GPS operations. Section 5 provides an overview of GPS jamming and spoofing detection methods. Section 6 discusses countermeasures to GPS jamming and spoofing, including an analysis of the state-of-the-art in positioning and navigation in a GPS-disrupted environment. Finally, Section 7 provides conclusions and open research directions. This paper focuses on GPS positioning and navigation aspects and does not cover the timing aspects of GPS performance or alternative timing approaches in GPS-denied environments. Furthermore, this paper considers generalized GPS performance, focusing on positioning and navigation within UAS applications.

Many modern devices do not rely solely on GNSS systems such as GPS; they rely on multiple sensors working in conjunction with GNSS for positioning and navigation. These sensors can sense the system's attributes, such as with inertial sensors, or the surrounding environment's attributes, such as with cameras. Data from these sensor systems are fused with GNSS-based data using methods such as a Kalman filter. Other systems utilize multiple GNSS systems, including GPS, GLONASS (Russian GNSS), Galileo (European GNSS), and Beidou (Chinese GNSS). The loss of GPS does not represent a complete loss of navigation data in multi-sensor or multi-GNSS systems but rather represents the loss of a single data source that could cause performance degradation to positioning and navigation solutions.

This paper extensively discusses various sensors and associated algorithmic methods used for positioning and navigation instead of providing a comprehensive examination of all components within a complex multi-sensor or multi-GNSS navigation system; however, its primary focus lies in GPS-denied scenarios, exploring these sensors and methods as strategies to counter GPS vulnerabilities and ensure reliable positioning and navigation even under compromised GPS conditions.

2. Existing Surveys

Several surveys related to GPS performance, GPS security, and navigation and positioning in GPS-denied and GPS-disrupted environments can be found in the literature. Table 1 lists recent surveys related to positioning and navigation in GPS-denied environments, emphasizing UAS applications, and specifies the topics covered and not covered by each of these surveys.

Table 1. High-level summary of the existing research on the topic of GPS security and alternate positioning.

Survey Paper	Topics Covered			Specific Topics		
	Attacks	Detection	Mitigations	GPS Spoofing	GPS Jamming	Alternative (Non-GNSS) Positioning and Navigation
[1]	X	X	X	X		
[2]	X		X		X	
[3]	X			X		
[4]	X	X	X	X		
[5]	X		X		X	
[6]	X		X		X	
[7]	X	X	X	X	X	
[8]	X	X	X	X		
[9]	X	X	X	X		
[10]	X	X	X	X		
[11]						X
[12]						X
[13]						X
[14]						X
[15]						X
[16]						X
[17]						X
[18]						X
[19]						X
[20]						X
[21]						X
[22]						X
[23]						X
[24]						X
[25]						X
[26]						X
Our paper	X	X	X	X	X	X

These surveys are analyzed in terms of (1) type of attack, (2) attack detection method, and (3) attack mitigation approaches. The papers were categorized according to the final topics: (1) GPS spoofing, an attack type where a malicious actor attempts to broadcast a falsified GPS signal to trick a receiver into calculating an incorrect position; (2) GPS jamming, an attack type where a malicious actor attempts to broadcast an interference signal to prevent a receiver from properly receiving the actual GPS signal; or (3) alternative (non-GNSS) positioning and navigation, such as positioning methods in GPS-denied environments. The authors of [1–4] provided a holistic review of literature focused on the UAS cybersecurity space, encompassing general aspects related to UAS cybersecurity, including GPS jamming and spoofing. They also analyzed the overall cybersecurity challenges facing unmanned systems, covering a broad range of threats to the various sub-systems that comprise these systems. The authors of [5] provided a comprehensive overview of jamming attacks and mitigation strategies across a wide range of wireless technologies, including GPS receivers. The authors of [6] focused on GPS jamming, summarizing different types of attacks and mitigation approaches. The authors of [7] presented a comprehensive review of unintentional and intentional threats against GNSS systems, focusing on GPS, discussing various degradation mechanisms, attacks against the GPS system, and many types of mitigations. The authors of [7] assessed the impacts of various types of degradation in terms of accuracy, integrity, availability, and continuity. Mitigation strategies were analyzed in terms of performance, cost, and complexity. The authors of [8–10] presented comprehensive reviews of GNSS spoofing threats, focusing on GPS. There is overlap between these surveys in the approaches they summarize, but they use different attack and mitigation taxonomies, which reflect slightly different foci between these papers. The authors of [8] proposed a taxonomy of spoofing mitigation methods consisting of (1) signal processing-based methods, (2) encryption-based methods, (3) correlation-based methods, and (4) antenna-based methods. The authors of [9] used a different spoofing mitigation taxonomy, dividing approaches into (1) signal processing-based approaches, (2) encryption-based approaches, (3) drift monitoring-based approaches, (4) signal geometry-based approaches, and (5) multi-pronged spoofing defense approaches. The authors of [10], primarily considering UAS applications, focus primarily on different types of GPS attacks. However, the authors of [10] provide a summary of many methods to make receivers robust against spoofing attacks, including a variety of approaches based on GPS signal characteristics and the perceived source location of the GPS signal. The authors of [10] also discuss the potential benefits of multi-GNSS receivers to mitigate GPS spoofing attacks.

The other survey papers [11–26] described non-GPS methods of positioning and navigation. There are many surveys on navigation and positioning in GPS-denied and GPS-disrupted environments; however, these surveys typically focus on the narrow aspects of positioning and navigation based on specific sensor types or methods. Many surveys focused on aspects of Simultaneous Location and Mapping (SLAM), discussing how autonomous systems learn and map an area while determining position within that area. SLAM most commonly uses some combination of optical sensors, such as cameras and Light Detection and Ranging (LiDAR) sensors. Many papers in the literature focused on the visual methods of positioning, where a system uses a camera to detect known landmarks within its surrounding environment. Other surveys focused on Inertial Measurement Unit (IMU)-based positioning approaches, where sensors such as accelerometers and gyroscopes are used to track a system's motion to determine relative position. Other papers in the literature focused on RF-based methods of positioning and satellite-based (non-GNSS) approaches. Several surveys related to positioning in GPS-denied environments focused more on summarizing the approaches found in the literature and did not provide a performance analysis of the approaches, discuss research gaps, or provide recommendations for future research directions. Table 2 provides a summary of those surveys that focused on positioning and navigation in GPS-denied environments and categorizes these papers in terms of the type of survey, creating a taxonomy with three high-level categories: (1) summarizing approaches in the literature on positioning and navigation in GPS-denied environments; (2) analyzing the effectiveness of alternative positioning and navigation methods; and

(3) providing insight into necessary research directions based on previous studies. These papers are also categorized by each survey's technical focus.

Table 2. Summary of alternate (non-GNSS) positioning and navigation survey papers.

Survey Paper	Type of Survey			Alternate Positioning and Navigation Methods Discussed in the Survey						
	Technical Approaches	Performance Analysis	Research Directions	RF-Based	Visual	Visual SLAM	Lidar-SLAM	Algorithm Evaluation	AI/ML Applications	IMU
[11]	X		X		X	X	X			X
[12]	X	X			X	X	X			
[13]	X	X			X	X			X	
[14]	X				X	X				
[15]	X	X						X		
[16]	X				X	X				
[17]	X					X				
[18]	X	X	X			X				
[19]	X	X				X				
[20]	X	X	X			X	X			
[21]	X						X			
[22]	X					X	X			X
[23]	X					X				X
[24]	X						X			
[25]	X	X				X			X	
[26]	X								X	
This paper	X	X	X	X	X	X	X	X	X	X

Visual SLAM, or vSLAM, has received the most attention in existing reviews. The authors of [11,12] provided comprehensive reviews of GNSS-independent navigation methods for autonomous vehicles, and further reviews of vSLAM methods are prevalent in the literature. Many vSLAM-focused reviews significantly overlap the techniques they discussed and simply present them within different taxonomies; however, several surveys focused on different aspects of vSLAM. The authors of [11] focused on assessing the technology maturity and reliability of various SLAM methods, including visual and laser-based approaches, with IMU sensor assistance for two-dimensional and three-dimensional mapping applications. The authors of [12] reviewed existing methods within a taxonomy of map-based navigation, where a region's map is known a priori and the system must determine its position within the known map, and mapless navigation, where little-to-know information about the region is known a priori. The authors of [13] presented one of the few reviews that discuss absolute visual localization (AVL) techniques, with a focus on UAS applications. AVL techniques provide absolute location in the form of latitude and longitude instead of relative location within some arbitrary reference system. Most existing surveys focused on relative visual localization (RVL) methods, in which the system's location is only determined within a non-absolute reference system, typically relative to other objects or waypoints. The core issue surrounding RVL is error accumulation, also known as drift over time. This issue can be somewhat alleviated through IMU-based enhancements; however, these approaches do not correct the underlying problem or applications that require long-term precision positioning. The authors of [14] discussed approaches for specific functions within the overall vSLAM problem space, including obstacle detection, obstacle avoidance, and path planning, within the context of mapless navigation approaches such as performing navigation, without a known map, map-based navigation approaches, and map-building approaches. The authors of [15] focused on summarizing various path planning and obstacle avoidance algorithms from the literature, comparing the performance of various algorithms in terms of computational efficiency and the optimality of solutions for several scenarios and obstacle layouts. The analysis presented by the authors of [15] demonstrated that certain algorithms performed better in certain scenarios; however, there were cases when they had higher computational time or less optimal solutions than other techniques. The proper choice of algorithm should be based on operational requirements to best balance computational time and solution optimality. The authors of [16] provided a review of vSLAM and generalized vision-based navigation, focusing on visual methods for (1) map-based navigation systems, (2) obstacle detection and avoidance approaches, and (3) path planning-based approaches, highlighting the strengths and weaknesses of the various approaches. Future research challenges identified include (1) the need for improved scalability, (2) improved computational efficiency, (3) improved algorithm reliability, and (4) improved algorithmic robustness.

Several vSLAM reviews discussed methods within a taxonomy based on the type of onboard visual sensor. The authors of [17] focused on approaches using monocular cameras. The survey discussed traditional visual SLAM methods, such as LSD-SLAM, ORB-SLAM, MSCKF, and DL-based methods. The authors stressed the difficulties of achieving real-time capability in vSLAM approaches and pointed out several key research directions in visual SLAM, including (1) the need for combined approaches that utilize IMU-based techniques, (2) the need for more work in incorporating DL-based techniques, and (3) the necessary mitigation of feature dependence, which the authors argue is the greatest limitation of vSLAM. The authors of [18] created one of the most comprehensive vSLAM reviews found in the literature, summarizing vSLAM methods across different types and numbers of visual sensors, including monocular vSLAM, stereo vSLAM, and RGB-D vSLAM. The authors also discuss different vSLAM methods, including event-based vSLAM, multi-modal vSLAM, and visual–inertial SLAM. They categorize vSLAM systems into three types based on how they use information from images: (1) direct or dense methods, (2) feature-based methods, and (3) semantic scene understanding methods. Each of these methods is described in detail, and various approaches are presented and discussed. The authors of [19] presented a brief survey of vSLAM methods, focusing on monocular techniques and presenting a qualitative and quantitative performance comparison of three of the most prominent algorithms in the literature: ORB-SLAM2 (sparse feature-based method), LSD-SLAM (semi-dense direct method), and DSO (sparse direct method). The algorithms demonstrated good performance; however, monocular approaches are susceptible to lens flare, overexposed images, water reflections, and moving objects and should be supported by other sensors, such as an IMU.

Many reviews discussed individual vSLAM [18] or Lidar-SLAM [11] methods; however, they focused on multi-sensor fusion methods, where multiple orthogonal sensor outputs were fused to estimate position information. The authors of [22] reviewed vSLAM and LiDAR-SLAM approaches combined with IMU-based methods. The multi-sensor fusion techniques discussed include visual–inertial approaches, LiDAR-inertial approaches, visual-LiDAR approaches, and LiDAR-visual–inertial approaches. The authors identified several critical future research directions, including the need for a versatile and efficient sensor fusion framework, additional DL-aided methods, and distributed cooperative methods. The authors of [23] surveyed multi-sensor fusion methods combining vSLAM with IMU sensors and proposed a modular multi-sensor data fusion technique. The authors of [20] considered LiDAR SLAM and vSLAM, along with multi-sensor methods such as LiDAR-vSLAM, visual–inertial SLAM (VI-SLAM), and LiDAR-inertial SLAM. These SLAM methods were considered for different sensor types, such as monocular vs. stereo. The authors of [10] provided a comprehensive review of visual and LiDAR-based SLAM techniques and approaches, considering map and mapless approaches that perform tasks such as obstacle avoidance, path planning, and map generation. They discussed some methods that also incorporate IMU-based measurements together with visual and LiDAR methods. The authors of [24] reviewed LiDAR-based SLAM techniques, considering both 2D and 3D LiDAR-SLAM approaches, and described the technical challenges of 3D LiDAR-SLAM, specifically the typical low vertical resolution and sparse point clouds associated with LiDAR. They concluded that multi-sensor fusion methods are required. The general benefits of multi-sensor fusion approaches were discussed, focusing on inertial-aided LiDAR-SLAM and visual-aided LiDAR-SLAM.

Several reviews focused on using Artificial Intelligence (AI) and machine learning (ML) in vSLAM and Lidar-SLAM. The authors of [25] provided a brief survey of vSLAM with a focus on deep learning (DL)-based methods, pointing out four key advantages of DL-based approaches to vSLAM compared with traditional approaches, which they broadly categorized as feature point methods or direct methods. First, DL methods had good invariance to illumination changes compared with traditional approaches. Second, DL-based vSLAM approaches could better identify moving objects in images than traditional approaches. Third, high-level semantic information could be extracted through DL to provide better context and understanding in map creation. Last, DL-based approaches removed the need for hand-constructed feature generation, widely understood as a general strength of DL approaches in any application. The authors discussed many of the DL approaches that researchers have already incorporated into the overall visual SLAM system, including the VO, the closed-loop detection process, and the semantic SLAM module, highlighting the performance benefits of these methods in dynamic environments. The authors of [26] also focused on AI-based approaches for UAS navigation. The techniques highlighted in [26] employed various types of optimization-based approaches, including genetic algorithms (GA), particle swarm optimization (PSO), ant colony optimization (ACO), simulated annealing (SA), pigeon-inspired optimization (PIO), Cuckoo Search (CS) algorithms, Dijkstra's Algorithm, Differential Evolution (DE), and Grey Wolf Optimization (GWO). The authors of [26] also discussed various DL-based approaches, including reinforcement learning (RL) and deep reinforcement learning (DRL). These algorithmic approaches can be applied to any navigation-related problem; however, the survey focused on path planning and optimization applications. The authors identified federated learning (FL) as a top future research direction, where AI model training occurs in a distributed manner across multiple devices using local datasets. Additional identified future research directions included the need for improved energy consumption, reduced computational power requirements, improved fault handling, and the need for AI-based solutions for physical threat avoidance.

The primary contribution of this paper is that we cover all aspects of Tables 1 and 2. There are many high-quality surveys in the literature; however, they typically focus on niche areas of the problem space. This paper covers all relevant aspects of GPS security, including threats, attack detection, and attack mitigation for jamming and spoofing. This paper also comprehensively describes positioning and navigation in GNSS-denied environments.

3. GNSS Overview

3.1. GPS System

The GPS constellation comprises 31 satellites operated by the United States Air Force (USAF). The first GPS generation achieved full operational capability in 1995 and has been subsequently modernized with GPS Block III satellites, which began launching in 2018. GPS works through a process known as trilateration, where the location of one point in space can be determined by the known characteristics of at least three other points in space. Each GPS satellite transmits a unique signal that can be received by a GPS receiver on Earth's surface. Embedded in that unique signal are the satellite's current location and the absolute time that the satellite transmitted the message. The GPS receiver then estimates how long the message took to travel from the satellite to the receiver, providing the receiver with an estimate of the distance between itself and that satellite. A 2D position estimate can be calculated once the distance is estimated from at least three satellites. A 3D position estimate can be calculated with range estimations from at least four satellites through a process known as trilateration. Figure 1 depicts the GPS trilateration process.

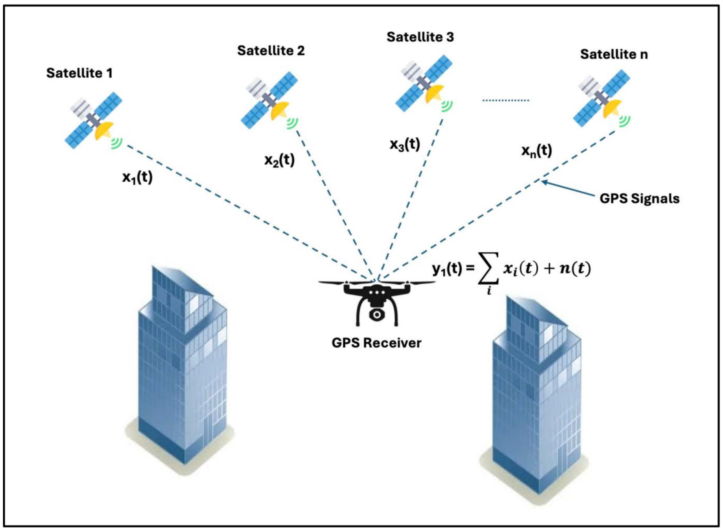


Figure 1. GPS trilateration for position estimation.

GPS satellites broadcast multiple downlink signals, including the L1 and L2 carriers operating at 1575.42 MHz and 1227.60 MHz, respectively. Newer GPS satellites also broadcast additional carriers, such as the L2C, L5, and L1C carriers. The L2C carrier was introduced in 2005 and gets its name from the frequency it uses (1227 MHz, the same as L2) and the fact that it is intended for civilian use. The L2C carrier is broadcast at a higher power than the L1 carrier, with the goal of better penetration through trees and buildings. The L2C carrier, sometimes referred to as the second civil signal, began broadcasting civil navigation (CNAV) messages in 2014; however, the USAF still considers L2C to be pre-operational. The L5 carrier, the third civil signal, is broadcast at 1176 MHz and was first introduced in 2010, with CNAV messages broadcast beginning in 2014. The L5 carrier is reserved exclusively for aviation safety services and features higher power and an advanced signal design for increased robustness compared with other carriers. L5 is still considered pre-operational by the USAF. The L1C carrier, referred to as the fourth civil signal, is broadcast at 1575 MHz and was originally designed as a common civil signal for GPS and Galileo. This carrier was designed to improve mobile reception in urban environments. Other GNSSs, such as BeiDou, are adopting similar signals. The first GPS satellites capable of broadcasting L1C were launched in 2018; however, L1 and L2, now known as the GPS legacy signals, remain the most common carriers supported by all PS satellite generations. There is also an L3 carrier at 1381.05 MHz, which is not used for navigation purposes. This carrier is used by the United States Nuclear Detonation (NUDET) Detection System (USNDS) to detect and locate nuclear detonations in the Earth's atmosphere and is used primarily for enforcing nuclear test ban treaties. The GPS signal is a spread-spectrum signal that simultaneously transmits multiple types of ranging and navigation messages. The GPS employs the Binary Phase Shift Keying (BPSK) digital modulation scheme for transmission. Some GPS satellites also employ a form of Quadrature Amplitude Modulation (QAM).

Each GPS satellite has several identifiers that are conveyed via ranging and navigation messages, including the space vehicle number (SVN), the space vehicle identifier (SVID), and the pseudorandom noise number (PRN). The PRN identifies which range code the satellite is using. A fixed unique mapping exists between the SVN, SVID, and PRNs described in the GPS interface specification [27]. The L1 and L2 carriers carry Course Acquisition (C/A) PRN codes, which are Gold codes transmitted at a rate of 1.023 Mbps and repeated every one millisecond. These C/A codes are exclusive or'd with a 50 bps navigation message containing information on the time and the satellite's position. Each satellite's unique PRN code is orthogonal to all other PRN codes, meaning each PRN code will not correlate with any other satellite's PRN code. Each C/A code chip corresponds to 293 m of distance; therefore, the receiver tracking this code will result in a range estimation no worse than 293 m and better in most cases. The Precision Code, or P-code, is a sequence of 6.187104 × 10^{12} chips transmitting at a rate of 10.23 million chips per second (Mcps) and repeating once a week. Receivers can use the C/A code for course range estimation and the P-code for higher resolution range estimation.

The original (legacy) GPS signal and messaging structure are depicted in Figure 2 [28]. The L2 carrier also has a W-code that is applied to the P-code at approximately 500 bps, the details of which are secret. This code is meant for US military usage; however, modern two-channel commercial GPS receivers can also track the L2 signal without knowing the W-code. These commercial receivers are more expensive and uncommon in consumer applications. A secure M-code in newer Block III GPS satellites is used for military applications that aim to improve the anti-jamming and secure access of military GPS signals.

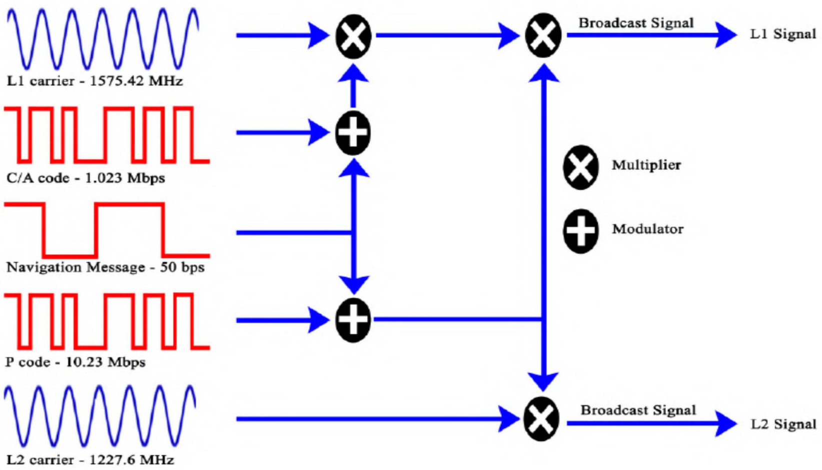


Figure 2. Legacy GPS signaling and messaging structure.

Receivers will demodulate the BPSK signal and process the NAV message to determine the time and location of the transmitting satellite. The receiver can then estimate the transmission delay and consequently estimate the range of the satellite. The receiver can estimate its 3D position once it can receive at least four satellite transmissions and estimate the range of each satellite.

GPS receivers utilize different aspects of the GPS signal to estimate range and position. Receivers utilize two primary observables to estimate the distance between the satellite and receiver: (1) code and (2) phase. The process previously described is code-observable; however, accessing the NAV message does not generally yield highly accurate results. This level of accuracy may be sufficient for some applications; however, additional precision can be obtained through the phase observable, where the unmodulated carrier phase is estimated by the receiver. Receivers can use the Doppler shift as another observable. The type and sophistication of processing vary across receivers based on several factors, including the required accuracy and desired cost point.

The position estimate is presented as its solution, along with several metrics that convey confidence in that estimate once the receiver has processed the signals. The receiver provides the Dilution of Precision (DOP) metric and is intended to reflect the quality of the satellite geometry and the resulting data uncertainty. Position DOP (PDOP) is another key metric that reflects the uncertainty of the overall position estimate. Horizontal DOP (HDOP) and Vertical DOP (VDOP) reflect the uncertainty in the horizontal and vertical components of the 3D position estimation. Higher values of DOP and PDOP generally mean a more accurate position estimate. DOP and PDOP typically increase as the number of visible GPS satellites increases, such as when the number of GPS satellites for which the signal can be successfully demodulated and processed increases, the geometry of the GPS satellites is more advantageous, and GPS receive signal strength (RSS) is higher.

3.2. Other GNSS Systems

While GPS is the oldest and most mature GNSS system, there are other GNSS systems that have emerged since the GPS system was initially fielded. The first is the Russian Federation's GLObalnaya Navigatsionnaya Sputnikovaya Sistema (GLONASS), with the first satellites launched in 1982 and reaching full operational capability in 1995. GLONASS consists of 24 satellites in medium-earth orbit (MEO). The constellation operates in three orbital planes, with eight evenly spaced satellites on each plane. For a GLONASS receiver to calculate an accurate position estimate, the receiver must be in range of at least four satellites. providing the system originally. GLONASS satellites broadcast two types of signals: (1) an open standard-precision signal and (2) an obfuscated high-precision signal available only to authorized users. The L1 and L2 carriers utilize Frequency Division Multiple Access (FDMA), where individual satellites transmit at slightly different frequencies. The most common GLONASS signals, L1 and L2, are centered at 1602 MHz and 1246 MHz, respectively, with both standard-precision and obfuscated high-precision signals provided at both L1 and L2. Starting with newer GLONASS-K1 satellites, a new L3 channel centered at 1207 MHz was introduced, which is also available on modern GLONASS-M+ satellites launched in the past decade. Similar to GPS, GLONAS uses Code Division Multiple Access (CDMA) and BPSK modulation. New CDMA-based signals have also been defined for L1 and L2 channels that are available in the newest GLONASS-K2 satellites.

Galileo, developed and maintained by the European Space Agency (ESA), is the European Union's (EU's) GNSS that consists of 28 satellites, all but two of which are positioned in three MEO orbital planes. The remaining two satellites were placed in incorrect orbits and are currently used for search and rescue purposes only but are not considered an operational part of the constellation. Galileo began providing an initial operational capability in late 2016. It broadcasts signals in three primary bands: E1, E6, and E5ab. The E1 carrier offers open service (OS) using a composite binary offset carrier (CBOC) modulation designed for reduced ranging noise and enhanced multipath performance. This E1 OS signal was also designed to provide improved interoperability with other GNSSs, sharing a common spectrum with the GPS L1C and BeiDou-3 B1C carriers. Dual-frequency receivers can also utilize the E5a and E5b signals, which share the same spectrum as the GPS L5 and BeiDou B2a carriers. The E5a and E5b carriers utilize an Alternative Binary Offset Carrier (AltBOC) modulation and multiplexing scheme. The E6 carrier includes a fully encrypted signal component for authorized users.

The Chinese BeiDou-3 system provides global GNSS service through its 24-satellite constellation in MEO across three orbital planes. Precedessor BeiDou systems (e.g., BeiDou-2) were regional systems and did not provide global service. BeiDou-3 began offering initial services in late 2018, with a full operational capability announced in 2020. This BeiDou-3 system offers four primary signals for navigation. The B1I and B3I carriers provide open services and were retained from BeiDou-2 for backwards compatibility. It also introduced the B1C and B2A carriers. B1C operates in the same spectrum as the GPS L1 and Galileo E1 carriers (1575.42 MHz), and the B2A carrier operates in the same spectrum as the GPS L5 and Galileo E5a carriers (1176.45 MHz). These spectrum choices were made to facilitate multi-constellation receivers. The BeiDou-3 system uses a range of modulation and multiple access approaches that are quite different than GPS, Galileo, or GLONASS systems. BeiDou-3 uses Constant Envelope Modulation via Intermodulation Construction (CEMIC) in the B1 band to generate the legacy B1I carrier. The B2A carrier is generated through Asymmetric Constant Envelope Binary Offset Carrier (ACE-BOC) modulation, while the B1C carrier uses Quadrature Multiplexed BOC (QMBOC). A unique feature of BeiDou-3 is the introduction of inter-satellite crosslinks that are capable of providing ranging measurements both within and across satellite orbital planes. This capability aims to reduce orbital errors, mitigate stale ephemeris, and consequently provide enhanced accuracy.

While there are many key differences between these various systems, the operating principles are similar. They are all predicated on a receiver estimating the range between itself and each observable satellite and using that information to generate its self-position estimate. Each system has code observables, phase observables, and Doppler frequency observables. For more discussion about the subtle differences between these systems in terms of design choices and services offered, the authors of [29,30] provide an overview and comparison between several of these systems. Note that the authors of [29] limit their comparison between GPS and GLONASS, while the authors of [30] consider all four of these systems. Figure 3 shows the spectrum of these various systems relative to one another [30].

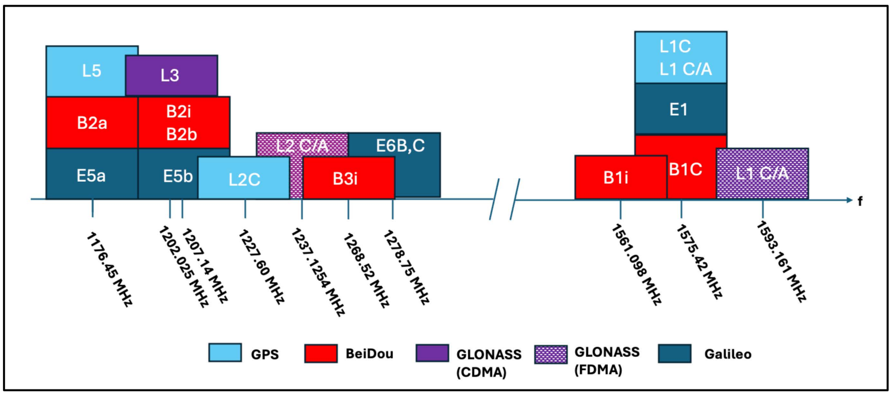


Figure 3. Spectrum allocations for worldwide GNSS civilian navigation signals.

3.3. GNSS Performance Expectations

GNSS positioning accuracy can vary based on receiver complexity, such as the type of signal processing; variation in receiver quality, such as hardware quality; environmental conditions; location; time of day; and geometry. GNSS receivers actually do not determine a range to each satellite but rather a pseudorange, which is just an estimate of range. Ideally, this pseudorange, $\widetilde{\rho}$, would match the actual range to the satellite, ρ, and would be a function of the speed of light, c, the time, t_R, and the time of the transmitter clock, t_T, such that $\widetilde{\rho} = c(t_R - t_T) = \rho(t_R, t_T)$ [31]. However, in practice, this range estimation varies from the actual range due to a variety of degradation factors, including atmospheric effects, multipath propagation effects, clock errors, Earth tides, and relativistic effects, among other noise terms. Because of these various degradation factors, the pseudorange observable takes the following form [31]:

$$\widetilde{\rho} = \rho(t_R, t_T) - c(\delta t_R - \delta t_T) + \delta_{IONO} + \delta_{TROPO} + \delta_{TIDE} + \delta_{PATH} + \delta_{REL} + \varepsilon \tag{1}$$

where

δt represents clock errors;
δ_{IONO} and δ_{TROPO} represents atmospheric effects of the ionosophere and troposphere;
δ_{TIDE} represents errors introduced by Earth's tidal cycles;
δ_{PATH} represents errors introduced by multipath propagation;
δ_{REL} represents relativistic errors;
ε represents all other unmodeled error sources [31].

Clock errors can be present on the satellite or receiver and can be caused by ephermis errors, receiver clock drift and bias, and measurement error. Ionospheric delay is a function of electron density along the signal's propagation path. Tropospheric delay is a function of environmental conditions along the signal's propagation path, such as temperature, barometric pressure, and humidity. Trophospheric propagation also introduces signal attenuation based on conditions. Multipath fading introduces delays due to signals traveling different propagation paths and can also lead to large-scale and/or small-scale fading (i.e., constructive and/or destructive combining at the receiver of signals taking different propagation paths). Other sources of error can include factors such as receiver noise, external noise/interference, and other propagation effects (e.g., blockage) that reduce the quality of the received signal.

As previously mentioned, some GNSS receivers make carrier-phase measurements of the GNSS signal to gain higher precision than is available through the code observable. However, there are error components that arise in this measurement. Two issues surrounding phase measurement are (1) phase ambiguity and (2) cycle slip. Phase ambiguity is due to the fact that adding integer multiples of the signal cycle will result in exactly the same measured phase. There are numerous methods that deal with phase ambiguity in GNSS receivers. But generally, these receivers do not distinguish between carrier cycles and generally measure fractional phases and then track phase changes. GNSS receivers will attempt to estimate an unknown initial ambiguity from the GNSS data. However, errors are generally present in the phase measurement. Cycle slip refers to the need for GNSS receivers to continually track signal phase; intermittent outages (e.g., signal shadowing) will change the value of the phase ambiguity. In this case, carrier phase tracking must start over, and there will be a period of time with degraded performance.

If there are no errors and no propagation effects, the measured phase, Φ, will take the following form [31]:

$$\Phi = \Phi_R(t_R) - \Phi_T(t_R) + N_R^T \quad (2)$$

where

Φ_R is the phase of the receiver;
Φ_T is the phase of the received satellite signal;
N_R^T is the ambuiguity between the satellite and receiver.

However, as was the case in the previous pseudorange discussion, the measured phase will differ due to several degradation factors, and the carrier phase measurement model will take the form of Equation (3) [31].

$$\lambda\Phi = \rho(t_R, t_T) - c(\delta t_R - \delta t_T) + \lambda N_R^T - \delta_{IONO} + \delta_{TROPO} + \delta_{TIDE} + \delta_{PATH} + \delta_{REL} + \varepsilon \quad (3)$$

where λ is the signal wavelength, and the remainder of the terms are similar to those in Equation (1). For a more thorough description of the various pseudorange and carrier phase measurement models and error components, the reader is referred to [32].

GPS Performance

The formal GPS performance standard published by the United States Department of Defense (DoD) [33] states that "[...] well-designed GPS receivers have been achieving horizontal accuracy of 3 m or better and vertical accuracy of 5 m or better 95% of the time". This level of accuracy has been substantiated by numerous studies, several of which are summarized in Table 3; however, these studies established variation due to the factors mentioned above.

Table 3. Summary of GPS performance analysis.

Authors	Reference	Type of Results	Scenario/Conditions Considered	Factors Considered	General Conclusions of Accuracy
U. Engel	[34]	Theoretical	Various	Clock error, orbit error, refraction, multipath, code-tracking error	Position accuracy: 5–30 m
M. Rychlicki et al.	[35]	Experimental	Open stationary, open mobile, urban stationary	Variability across GPS receivers	HDOP: 0.7–1.2 VDOP: 0.9–1.6
J. Salas and M. Torroja	[36]	Experimental	Open stationary, open mobile	Variability across GPS receivers	Position accuracy: 0–4 m
M. Modsching et al.	[37]	Experimental	Urban stationery	Variability across GPS receivers	Position accuracy: <28 m for 95% of the time

Table 3. *Cont.*

Authors	Reference	Type of Results	Scenario/Conditions Considered	Factors Considered	General Conclusions of Accuracy
P. Misra et al.	[38]	Theoretical, experimental	Various	Geometry, number of satellites, ranging errors, types of receiver signal processing and hardware	Position accuracy: 0.01–30 m
R. Conley	[39]	Theoretical	Various	Location on Earth, various error sources	Variable: centimeters to 10's of meters
J. Spilker Jr.	[40]	Theoretical	Various	Various	Position accuracy: <10 m
D. Skournetou and E. Lohan	[41]	Theoretical	Open	Single vs. multi-frequency receivers	Ranging accuracy: 10–100 m
K. Merry and P. Bettinger	[42]	Experimental	Urban stationery	Multipath propagation	Position accuracy: 7–13 m
K. Chiang et al.	[43]	Theoretical, Experimental	Urban stationary, urban mobile	Multipath propagation	Position accuracy: <5 m
A. Hussain et al.	[28]	Theoretical	Urban stationary, urban mobile	Multipath propagation	N/A—Focus on detection and acquisition of GPS signals

N/A: Not Applicable.

Multi-frequency GPS receivers processing both L1 and L2 carriers can obtain improved position accuracy with centimeter-level accuracy [41]; however, as previously noted, multi-frequency GPS receivers are larger, more expensive, not common in consumer or commercial applications, and are historically more prevalent in professional and military applications.

There is also the concept of Differential GPS (D-GPS). D-GPS is based on the idea that two receivers near each other experience similar atmospheric errors. A network of GPS receivers at known locations is established, and they publish their signal measurement data for each visible satellite for public consumption. GPS receivers can then download this information, commonly referred to as GPS correction data, from the nearest fixed site and apply that data to correct any measurement errors in their data, improving the accuracy of their position estimation. This process can be done in real time if the GPS receiver can access the required connectivity. More commonly, differential correction is performed in non-real time by post-processing the published correction data.

4. Factors Contributing to GPS-Denied or GPS-Disrupted Environments

Several factors can contribute to GPS degradation or disruption, either intentionally through malicious attacks or unintentionally from unintended interference or propagation-related degradation. These factors include multipath fading, signal shadowing, unintentional interference, jamming, and spoofing. These various degradation factors have different degrees of implementation difficulty, require different levels of hardware and software complexity, and require varying levels of technical expertise to implement, making different attack scenarios more likely. Additionally, these various degradation factors have key differences in terms of potential effect, scope of the potential effect, and different potential ramifications. The various types of GPS degradation factors and their key characteristics are summarized in Table 4.

Table 4. Summary of GPS degradation factors.

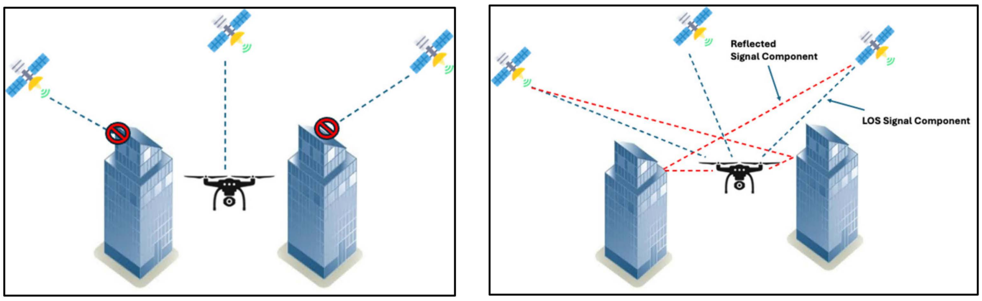
GPS Degradation Factor	Summary	Difficulty of Implementation	Required Expertise	Likelihood	Effect	Scope of Effect	Possible Ramification
Multipath Fading/Shadowing	Complex urban environment degrading GPS reception	N/A—natural condition	N/A—natural condition	High	Performance degradation or total GPS signal loss	Localized to urban centers	GPS-based navigation is not possible or causes crashes or impacts due to position error
Unintentional interference	Unintended emissions in GPS frequency bands	N/A—unintended action	N/A—unintended action	High	Performance degradation or total GPS signal loss	Localized to sources of interference	GPS-based navigation is not possible or causes crash or impact due to position error

Table 4. *Cont.*

GPS Degradation Factor	Summary	Difficulty of Implementation	Required Expertise	Likelihood	Effect	Scope of Effect	Possible Ramification
Jamming	Intentional emissions in GPS frequency bands	Very low—can be implemented with low and no-cost commercial hardware and software	Low—basic SDR, RF hardware, and software development expertise or low-cost commercial jammer	High	Performance degradation or total GPS signal loss	Localized-to-wide area of effect	GPS-based navigation is not possible or causes crashes or impacts due to position error
Spoofing	Intentional broadcast of falsified GPS signal	Very low—low and no-cost commercial hardware and software	Low—basic SDR, RF hardware, and software expertise	High	GPS receiver reports an incorrect position	Localized-to-wide area of effect	Vehicle under spoofer control—could lead to loss of property or life

4.1. Propagation-Induced GPS Degradation

The very low GPS power levels received at the Earth’s surface make the system sensitive to blockages and shadowing. This issue occurs when a manmade structure or natural terrain feature blocks the line-of-sight (LOS) from one or more GPS satellites to the receiver. The need for the precise propagation time estimation required to estimate receiver-to-satellite range for GPS trilateration also makes the performance sensitive to multipath fading propagation conditions. This problem occurs when the GPS signals reflect off manmade structures toward the GPS receiver. The reflected signal components will be delayed in time compared with the LOS signal component due to the longer propagation path taken, resulting in the GPS receiver receiving the LOS component of the GPS signal and these time-delayed reflected signals. These different time-delayed versions of the same signal can either constructively or destructively add at the receiver, depending on the geometry and environment, resulting in large-scale and small-scale signal fading. These degradation factors are problematic in both suburban and (particularly) urban settings. The “urban canyon” scenario, which describes the scenario within a large urban area with many tall buildings, has historically proved problematic for GPS signal reception. These propagation-induced degradation factors are depicted in Figure 4.



(**a**) (**b**)

Figure 4. Propagation-induced GPS degradation factors, including (**a**) signal shadowing and (**b**) multipath fading.

Several studies have investigated GPS performance in suburban and urban propagation environments; however, these studies do not typically isolate degradation due to shadowing or multipath fading. Instead, both shadowing and multipath fading are loosely categorized as urban propagation. GPS performance in complex urban environments has been the focus of study in several existing papers [35,37,42,43] with greatly varying reported results. The authors of [43] presented experimental results revealing position accuracies of less than five meters in a built-up urban environment, similar to those observed in the literature for open environments. The authors of [42] also observed good performance in an urban measurement campaign, with reported accuracies of 7–13 m; however, the authors of [37] observed much greater variability in position accuracy in urban environments. The authors of [37] concluded that location-based applications must assume a position error of at least 28 m within their application due to the effects of signal shadowing caused by nearby buildings.

The varying results reported in these research papers suggest that performance in urban environments is sensitive to environmental details and subject to high variability. These results could suggest that the precise effects of multipath fading and shadowing on GPS reception may not be easily generalized and might require study for specific regions of interest; however, other frequency bands and signals of interest, such as commercial cellular communications, have generalized channel models that are reasonable across a wide range of complex urban environments. These frequency bands have historically received significantly more interest, with thousands of papers published on cellular channel models and measurement campaigns; therefore, the lack of a high-fidelity generalized GPS urban propagation model may be due to insufficient research and publications. Researchers were in general agreement that urban canyon scenarios, such as very tall buildings in dense city downtowns, yield poor accuracy performance or total GPS signal loss.

One problem with all studies on this subject is the lack of experimental details and subsequent lack of reproducibility. The papers on GPS performance in urban environments do not give a sufficient description of the details of their experiments or their test environments. It is challenging to draw generalized conclusions or validate the results of these papers without these details. Furthermore, it is difficult to conclude what factors provide the largest contribution to the results without an attempt to isolate degradation factors, such as shadowing and multipath fading.

4.2. GPS Jamming and Unintentional Interference

GPS signals are extremely weak on Earth's surface, often on the order of -130 dBm or lower. A relatively low power emitter can interfere, intentionally or unintentionally, with proper GPS signal reception, exacerbated by the fact that commercial GPS receivers use varying-quality hardware components and signal processing methods, which can lead to poor performance for some receivers in non-pristine electromagnetic environments. Unintentional interference can be caused by malfunctioning or misconfigured equipment that emits energy into the GPS frequency bands. Unintentional interference can be caused by unsuppressed harmonic emissions into the GPS band or intermittent spurious out-of-band emissions from RF equipment. Unintentional interference can be difficult to detect or locate due to the highly temporal nature of the interference, especially if it is caused by mobile equipment or human activity. Intentional GPS interference, also known as GPS jamming, is typically one of four types: (1) barrage jamming, (2) continuous wave (CW) or tone jamming, (3) chirp jamming, and (4) protocol-aware jamming. Barrage jamming involves the transmission of noise across a wide bandwidth, covering the entire target signal's channel bandwidth. CW jamming focuses the interference energy into a very narrow bandwidth within the target signal's channel. Chirp jamming is an approach where the interference frequency changes rapidly over time. Chirp jammers are often narrowband; therefore, they resemble a swept-tone signal. Protocol-aware jammers attempt to utilize the target signal's attributes to optimize their jammer waveform.

There is wide agreement that GPS is susceptible to interference; however, only limited studies on the topic of GPS interference exist. The authors of [44] presented the results of a measurement campaign conducted across Europe over two months in 2016. The authors established eleven signal detection sites across seven European countries: the United Kingdom, Sweden, France, the Czech Republic, Poland, Slovakia, and Finland. Site locations included airports, near major roads, above motorways, busy city areas, and urban areas. Continuous spectrum monitoring and capture were conducted, and the resulting data were processed to determine interference events and attempt to classify the interference type. Over 5000 interference events were recorded over this period, with over 1000 classified as significant interference events, with positioning errors of hundreds of meters or complete GPS disruption near the receivers. The authors of [44] analyzed and identified the different types of interference events. Table 5 [44] summarizes the mean weekly occurrence rate for different types of measured interference events.

Table 5. Mean weekly number of different types of interference events from the measurement campaign presented in [44].

Location	AWGN Wideband	Narrowband Single-Tone	Chirp	CDMA	Other
Site 1	16.2	9.3	0.5	0.1	0.7
Site 4	37.3	4.8	1.2	0.8	0.5
Site 5	12.0	11.9	13.5	1.5	7.1
Site 7	12.9	43.1	2.8	1.1	1.8
Site 8	124.2	131.2	73.8	8.3	28.2
Site 9	10.0	3.7	3.5	0.5	11.0
Site 10	42.9	23.3	38.0	3.7	23.3

These various interference events had different durations and power levels. Many of these events were ultimately deemed unintentional interference, such as the wideband noise and narrowband signals in the two leftmost columns of Table 5. The detected chirp signals are likely from GPS jammers since chip signals are common for GPS jammers sold on the Internet (black market) [45,46]. The results of this type of measurement campaign vary across location and time; eleven randomly chosen locations had different results. Two important conclusions can be drawn from the results of this measurement campaign: (1) unintentional GPS interference is a common occurrence, and (2) intentional GPS interference, such as GPS jamming, is not a rare event.

A similar measurement campaign was performed by the authors of [47], primarily focusing on two locations in the Czech Republic over 140 days in 2021. During this time, 2158 interference events were reported, 872 of which were deemed high-impact events that caused GPS accuracy degradation or outages. One event was particularly interesting because it occurred simultaneously across both locations, which also strongly correlated to an interference signal recorded at test sites throughout Europe, including Belgium, France, Germany, Latvia, Finland, and the United Kingdom. This event was a narrowband interference signal located near the center of the L1 carrier and caused widespread GPS signal disruption or outage for several seconds. The estimated affected area was approximately one million square kilometers. Data were analyzed to determine if this event could have been caused by solar activity or some type of space weather event; however, the source of this interference remains unknown.

Several papers in the literature discuss the feasibility of implementing low-cost GPS jammer systems. For example, the authors of [48] presented a study examining the detection and jamming of small commercial UAVs through low-cost commercial GPS jammers. The authors of [45] described results from a study that implemented a GPS attack system against a DJI Phantom 3 quadcopter UAS utilizing low-cost, commercially available hardware and software. The authors used a BladeRF X40 software-defined radio (SDR) platform with signal generation performed within the GNU Radio SDR development environment. The authors of [49] utilized a similar jammer design as reported in [50], using a BladeRF x40 SDR platform and the GNU radio software environment. They implemented various jamming techniques, including barrage jamming, CW tone jamming, sweeping noise jamming, sweeping narrowband pulse jamming, and a protocol-aware jamming waveform that matched the characteristics of the GPS signal structure. The authors of [51] demonstrated an SDR-based GPS jammer developed within GNU Radio. The authors of [52] also demonstrated an SDR-based GPS jammer developed using a BladeRF X40 SDR and GNU Radio. The results of [48] through [49] revealed that effective GPS jammers can be constructed using low-cost commercial (typically black market) GPS jammers or low-cost

SDR hardware and software components. Effective GPS jamming systems are not difficult to implement using low-cost and no-cost open-source components. Table 6 summarizes the various GPS jammer implementations found in the literature.

Table 6. Summary of low-cost GPS jammer implementations.

Authors	Reference	Difficulty of Implementation	Type of System	RF Hardware Platform	Signal Generation Environment
Farlik et al.	[48]	Low	Commercial	Commercial GPS Jammer	Commercial GPS Jammer
Saputro et al.	[50]	Low	SDR-based	BladeRF x40	GNU Radio
Ferreria et al.	[49]	Low	SDR-based	BladeRF x40	GNU Radio
Karpe and Kulkarni	[51]	Low	SDR-based	Unknown	GNU Radio
R. Ferreira et al.	[52]	Low	SDR-based	BladeRF x40	GNU Radio

A small number of papers quantitatively study the impact of jamming on GPS receiver performance. Most notable are the research efforts presented by the authors of [53,54]. The authors of [53] analyzed several different types of jamming against a simulated GPS waveform. They considered four different types of jamming strategies: (1) pulse jamming, (2) continuous wave (CW) jamming, (3) barrage noise jamming, and (4) swept partial-band noise (PBN) jamming. This study demonstrated that CW jamming results in the largest degradation of the GPS signal, closely followed by barrage noise jamming. BER performance asymptotically approached the BER rates as jammer power increased, likely due to the spread spectrum nature of the GPS signal. Further degradation was likely due to the saturation of the GPS receiver's RF front-end hardware. The authors did not consider chirp jamming, which is known to be highly effective against GPS. Table 7 summarizes the effectiveness of the different jammer strategies presented in this study [53].

Table 7. Summary of effectiveness of different GPS jamming strategies presented in [53].

Type of Jamming	Resulting BER (%)
Pulse Jamming	4–8%
CW Jamming	18%
Barrage Noise Jamming	14%
Swept PBN Jamming	2–4%

The studies presented in [54,55] provided insight into the performance variability of different GPS receivers in the presence of jamming. The authors of [54] presented an analysis of GPS performance against chirp jamming, commonly found in commercially available GPS jammers. The authors primarily considered linear chirp jamming against two GPS receivers and measured the corresponding GPS carrier-to-noise (C/No), DOP, and position solution accuracy. One of the test receivers was a multi-GNSS receiver; therefore, it was tested in GPS-only and multi-GNSS configurations. This study reported significant differences in performance between these GPS receivers, with some scenarios resulting in minimal error in one device and errors of up to 10 m in the other device. The authors also noted that the multi-GNSS configuration resulted in the best performance, with little-to-no performance degradation in the presence of GPS jamming. This result is expected since other GNSS systems, such as GLONASS, operate in different frequency bands, and the receiver always receives unaffected signals from at least one GNSS system. The authors of [55] conducted an empirical study of five different GPS receivers in the presence of jamming, attempting to gain insight into the variability of GPS receiver performance. This study presented the minimum jammer power levels required to make the different receivers lose GPS signal lock; however, the authors failed to describe the propagation path between the jammer and target receivers, and it is not possible to determine meaningful receiver metrics such as Signal Power to Jammer Power (S/J).

The data from [55] provided insight into the variability of GPS receivers in jamming conditions. The five GPS receivers that were tested required jammer power ranging from −45 dBm to −60 dBm to disrupt their GPS signal reception. These results suggest a 15 dB variability in S/J performance across the five tested GPS receivers, assuming receivers were collocated such that GPS signal power was comparable across all receivers. This variability is significant and suggests that different GPS receivers will respond significantly differently to a jamming signal or unintentional interference.

4.3. GPS Spoofing

Commercial GPS signals are not authenticated or protected from malicious attacks, including GPS spoofing, where an attacker broadcasts falsified GPS signals, allowing a receiver to believe they are in a different position. This type of attack is easy to generate due to the low signal strength of the downlink GPS signal, making it easier for the malicious attacker's signal to overwhelm the actual GPS signal at the receiver. This attack type is more relevant to the L1 carrier since it does not have any type of protection and is less relevant to the L2 carrier since the L2 carrier implements cryptographically protected codes. Consequently, this type of attack is more relevant to commercial and consumer GPS receivers.

There are a limited number of papers that discuss real-world examples of GPS spoofing attacks; however, the authors of [56] did provide a discussion of some real-world examples, such as the well-known "Iran-US RQ-170 incident", where Iranian forces captured a Lockheed Martin RQ-170 Sentinel UAS using a GPS spoofer in December 2011, which was publicly confirmed by the US military shortly after the event took place. The authors of [56] also discussed the work conducted by researchers from the University of Texas at Austin in 2013 and 2014. The authors built a GPS spoofer using low- and no-cost hardware and software components and then successfully spoofed a UAS and a ship. The spoofer caused the ship to travel in a zigzag motion while the ship's autopilot reported a straight line of travel. The authors of [57] described the results of experiments conducted to seize control of a UAS navigation system through GPS spoofing. They systematically analyzed how to transmit falsified GPS signals and then prevent detection to maintain UAS control. The authors of [58] presented research where they implemented a GPS spoofer and injected the spoofed signal into a GPS receiver embedded within a UAS testbed. That GPS receiver was not providing stand-alone navigation but was rather part of a fusion approach that combined GPS data with inertial sensors. The authors demonstrated that even in this multi-sensor fusion approach, GPS spoofing was effective and that the UAS testbed's navigation system was compromised. The study presented in [58] did not utilize an actual UAS but rather a testbed running the actual flight control software of a commercial UAS. So while the results must be caveated as such, these results still clearly illustrate the effectiveness of GPS spoofing.

GPS spoofers can be coherent, meaning they are phase and frequency synchronized with the actual GPS signal, or non-coherent, meaning they are not phase and frequency synchronized with the actual GPS signal. The authors of [59] presented a theoretical relationship between GPS spoofing signal synchronization error and required GPS spoofing signal power. The authors of [59] then provided practical advice and guidance on optimizing system design to GPS spoofing system designers. The authors of [60] also provided an analysis of potential GPS spoofer system design choices, focusing on potential techniques and strategies a spoofing system may employ in an attempt to minimize detection. Coherent GPS spoofing is more difficult to implement but can have a greater impact on the target receiver and requires stronger detection mechanisms within the receiver. The authors of [61] developed an advanced digital signal processor (DSP)-based GPS spoofer that was capable of high-fidelity civil GPS signal creation with significant carrier phase and Doppler frequency offset accuracy, such that the spoofed signal was virtually indistinguishable from authentic GPS signals. This work aimed to study the effectiveness of potential defense mechanisms against spoofing attacks. Many potential defenses were postulated;

however, the authors concluded that cryptographic authentication was required against a sophisticated spoofing attack.

Many studies have established that low-cost GPS spoofers can be implemented using commercial SDR hardware and open-source software. A wide variety of low-cost SDR units are available, such as the HackRF and BladeRF platforms, which are the most popular. There are also open-source signal generation environments that can be leveraged for GPS spoofing, such as the GPS-SDR-SIM GPS signal simulation software package. The authors of [62] presented research in which they constructed a low-cost GPS spoofing system using a HackRF One SDR platform connected to a laptop computer running the GPS-SDR-SIM GPS signal simulator. This GPS spoofing system was tested against a Holystone HS7000 UAS. The authors did not provide results in terms of effective range, but they did demonstrate that spoofed signals are effective. The authors of [50] also used their BladeRF X40 SDR-based system to implement a GPS spoofing attack. The authors of [63] constructed a GPS spoofer utilizing the BladeRF x40 SDR platform with the GPS-SDR-SIM GPS signal simulator. They tested this low-cost GPS spoofer against a Huawei tablet with a GPS receiver and demonstrated that the receiver reported the spoofed GPS position. The authors of [64] presented a low-cost GPS spoofing system based on the HackRF One SDR platform attached to a laptop computer running the GPS-SDR-SIM GPS signal simulator. They tested the effectiveness of this solution against a GPS-enabled smartphone, successfully demonstrating that their low-cost system transmitting a spoofed L1 GPS carrier caused the smartphone to report the incorrect spoofed position. The research presented in these papers clearly illustrates that an effective GPS spoofing system can be implemented easily and inexpensively. Table 8 summarizes low-cost GPS spoofer implementations found in the literature.

Table 8. Summary of low-cost GPS spoofer system implementations.

Authors	Reference	Difficulty of Implementation	Type of System	RF Hardware Platform	Signal Generation Environment
Satyanarayana et al.	[62]	Low	SDR	HackRF One	GPS-SDR-SIM GPS
Ueki et al.	[63]	Low	SDR	BladeRF x40	GPS-SDR-SIM GPS
Saputro et al.	[50]	Low	SDR	BladeRF X40	GPS-SDR-SIM GPS
Songala et al.	[64]	Low	SDR	HackRF One	GPS-SDR-SIM GPS
Karpe and Kulkarni	[51]	Low	SDR-based	Unknown	GNU Radio

There are several additional critical insights from existing research. First, unmanned systems can respond erratically and catastrophically to rapidly varying spoofed positions. The authors of [62] noted that a UAS exhibited erratic behavior, rapid speed increases, and a subsequent crash when a very low position altitude was rapidly spoofed. The authors of [65] discussed how rapid or erratic changes in the spoofed position could result in UAS crashes and proposed a GPS spoofing algorithm that implemented slow changes in the spoofed location to create the desired deception trajectory without adverse effects, such as crashing or detection. Second, a GPS spoofer's effectiveness depends on the quality of the authentic GPS signal. Experiments performed in [50] examined attacks against a GPS-enabled smartphone device in indoor and outdoor scenarios. The GPS spoofing system successfully tricked the receiver in both scenarios; however, spoofing took significantly longer outdoors.

In some cases, GPS spoofing did not become effective until approximately three minutes later. Spoofing was never effective when the actual GPS signal had a very high DOP. These results suggest that the effectiveness of GPS spoofing might be directly related to the signal's quality in terms of signal strength and system geometry. These results also suggest a temporal aspect to spoofer effectiveness. A spoofed GPS signal does not necessarily have to "overpower" the actual GPS signal to be effective. A key result from [63] is that position estimation error begins to grow if the spoofed GPS signal is 8.04 dB weaker than the actual GPS signal. The spoofed signal controlled the position once it was 4.52 dB weaker than the actual GPS signal. There is an example in the literature revealing the ease with which GPS timing information can be spoofed, such as when the GPS receiver has an accurate position but the attacker controls the absolute time information [66].

5. Detection Techniques and Their Comparison

The necessary first step in effectively mitigating performance degradation is reliably detecting that degradation mechanism. This section provides an overview of the detection mechanisms found in the literature for different types of GPS disruptions. We did not focus on propagation-induced GPS disruption; instead, we focused on detecting intentional attacks on GPS receivers, GPS jamming, and GPS spoofing. Some of the existing research efforts can apply to multipath-induced GPS disruption and unintentional interference scenarios.

5.1. GPS Jamming Detection

Most commercial GPS receivers do not have anti-jam or jamming detection features; however, there are some examples of commercial products that have jamming detection features. The authors of [55] presented a study evaluating the performance of various GPS receivers in the presence of jamming. One of the devices, the u-blox NEO-6 GPS receiver, was equipped with jamming detection capability. The NEO-6 provides a jamming level estimator (the jamIND field in the MON-HW message) that is intended to assess the likelihood of an ongoing jamming attack. A higher value indicates that a jamming signal is likely present. A narrowband jammer signal near the L1 center frequency interfered with the receiver and disrupted navigation; however, the NEO-6 reported an extremely low probability of a jamming attack. This result is unsurprising given the low-cost nature of most commercial GPS receivers. Existing commercial jamming detection capabilities are unlikely to perform well.

There is significant research on GPS jamming attack mitigation; however, there are far fewer papers on GPS jamming detection. Historically, simple energy detection and thresholding have been used for jammer detection. This approach works well for high-power jammer systems; however, energy-based approaches do not perform as well when the incident jammer energy is comparable to the target signal energy. Some of the papers that proposed GPS jamming mitigation approaches also embedded a form of jamming detection as part of their overall approach, but generally, those approaches are not standalone in nature. Overall, existing GPS jamming detection methods appear to fall into one of three primary categories: (1) based on the statistical properties of the received signal, a derivative of energy-detection approaches; (2) based on antenna array hardware approaches; and (3) based on ML approaches.

Research has historically focused on the first two categories: statistical signal properties-based and antenna-based approaches. Newer proposed approaches have attempted to leverage ML-based approaches that can consider the GPS signal properties, the jammer signal, and the GPS receiver to support detection decisions. Open questions for these approaches are (1) how they perform in complex propagation environments, such as urban canyons, and (2) how they perform with GPS receiver equipment, given the variation in GPS receiver performance that has been demonstrated previously. Another consideration is the complexity of the proposed solutions and whether they are practical for small UAS platforms with limited computational capability. This question is particularly relevant for ML-based approaches and whether they can be computationally optimized to execute on unmanned platforms with low processing capabilities, small amounts of volatile memory, and limited persistent storage space. These approaches are summarized in Table 9.

5.1.1. Signal Statistics-Based Methods for Jamming Detection

Examples of these methods include using changes in signal strength, power spectral density, or other statistical properties to identify the presence of a jammer. The authors of [67] proposed a method to detect and classify the type of jamming signals based exclusively on the statistical properties of the power spectral density (PSD) for the overall received signal. The authors of [67] demonstrated that the PSD of the composite GPS plus jammer signal will take on different shapes and statistical properties. Specifically, the proposed approach attempted to characterize the range of maximum PSD amplitude values for the received signal and then used PSD amplitude to characterize jammer presence and type. The advantage of this approach is its simplicity and ease of implementation in real-world GPS receivers; however, certain jammer signal types, specifically swept noise jamming, have PSD characteristics like the GPS signal itself, which would appear to make it difficult to detect this jammer type. The method proposed in [67] also does not seem to account for propagation loss between the jammer and target GPS receiver. It is unclear how one would necessarily know the appropriate range of maximum amplitude values for the received jammer signal PSD without this knowledge. A similar approach was proposed in [68], where the statistical properties of the received signal spectrum were used to detect the presence of a jammer. The fundamental assumption in this approach was that the jammer caused any variations in the received signal's statistics. Using this assumption, substantial changes in PSD mean or variance would be attributed to the presence of a jammer. It is unclear how this approach will perform in complex multipath fading and signal shadowing environments, where significant receive signal fluctuations will occur with or without the presence of jamming. Additionally, these approaches may perform well for high-power jammers, but it is unclear how they will perform when the received jammer power is roughly equivalent to the GPS signal.

Table 9. Summary of common approaches for GPS jamming detection.

Type of Approach	Underlying Concept	Strengths	Key Open Research Questions
Signal Statistics-based	Monitor received signal attributes and attribute changes in statistical properties to jammer	Simple to implement, based on easily observable parameters	How will these approaches work in complex propagation environments?
Antenna-based	Utilize antenna array to measure aspects of signal to discern between authentic signals and jammer signals	Ability to jointly detect and mitigate interference	Can antenna arrays be made sufficiently simple to be viable for small platforms?
Learning-based	Fuse attributes of GPS signal, jammer signal, and GPS receiver into predictive ML model	Among the best performing approaches in open literature	Can ML models be sufficiently optimized to run on small platforms with limited computational capability?

The authors of [69] proposed a somewhat similar approach to detect the presence of a jamming signal based on the overall RSS in the L1 GPS band. BER was considered in the jammer detection approach. The underlying assumption was that a rapid change in RSS or BER was likely due to the presence of a jammer signal. The proposed approach monitored and created a time-series history of RSS and BER for the L1 band. Jammer detection was declared when a rapid increase in RSS and BER was detected. The results presented in [69] suggested very good detection performance for this approach; however, this approach may be limited in scope and may not perform well in multipath and shadowing propagation environments where the actual GPS signal level may be rapidly fluctuating. The research in [69] focused on the use case of an oceanic surface ship attempting to detect GPS jamming. The receiver would have clear visibility into the GPS satellite constellation and would not rapidly fluctuate in that environment. Consequently, it may be a reasonable assumption that any rapid increase in BER is caused by interference; however, this assumption may not hold true in a complex environment that produces multipath fading and signal shadowing. Rapid rises in BER could just as easily be caused by signal shadowing or destructive signal fading. Rapid rises in RSS could be the result of constructive signal fading.

A similar approach was proposed by the authors of [70], where a Moving Variance (MV) approach was proposed to detect the occurrence of jamming in the L1 band. This approach was predicated on the assumption that rapid variations in L1 carrier-to-noise (C/No) Density Power are likely attributable to a jammer. A rapid change in the sliding window statistics of the L1 C/No was used to declare the presence of a jammer. As in the case with [69], it is unclear how this approach will perform in dynamic and complex multipath and signal shadowing environments, where C/No will be rapidly fluctuating regardless of the presence of a jammer signal.

5.1.2. Antenna Array-Based Methods for Jamming Detection

These approaches generally rely on using some statistical property of the received signal combined with spatial processing to detect the presence of interference. The authors of [71] proposed an antenna array approach based on measuring the carrier phase differences of incoming signals. Specifically, the double difference of the carrier phases was used to detect the presence of a jammer. The double difference in the carrier phases of these two signals will be extremely small if a jammer generates two PN code signals because they were generated from the same platform and arrived at the receive antenna from the same direction. Two PN code signals generated by actual GPS satellites will arrive from different directions and have a much larger double difference. This procedure can be simply implemented by measuring the carrier phase of the incoming signal and comparing it with a value that would be representative of a jammer-generated signal. The authors of [71] reported good detection performance; however, this type of approach would require an antenna array, which is more complex than the typical patch antennas found in most commercial GPS receivers. It is unclear if this approach would be feasible for smaller, unmanned platforms.

5.1.3. ML-Based Methods for Jamming Detection

These approaches employ multiple properties of the received signal as features in a supervised ML model. The authors of [72] employed an ML approach to GPS jamming detection. A testbed was developed to generate synthetic GPS signals utilizing GNU Radio with a National Instruments B-210 Universal Software Radio Peripheral (USRP) both with and without the presence of a variety of types of jammer signals that were fed to a u-blox M8 GPS receiver. Four types of jamming signals were considered: barrage noise, single tone, successive pulse, and protocol-aware (P-aware). The authors then performed feature analysis to determine the most salient features in the resulting signal data, such as position accuracy, HDOP, and COP, and used those features for each dataset to train various types of ML models. The performance metrics included detection rate (DR), misdetection rate (MDR), false alarm rate (FAR), and F-score (FS). The authors established that a neural network approach yielded the best performance, with DR, MDR, FAR, and FS values of 98.9%, 1.39%, 0.28%, and 0.989, respectively. K-Nearest Neighbor (KNN) yielded similar performance but suffered from much longer prediction times. Random Forest approaches also performed well but experienced longer prediction times. Other approaches, such as Decision Tree (DT) and Support Vector Machine (SVM), yielded poor performance. This neural network approach is promising and may eventually yield a good, generalized solution to GPS jamming detection; however, an unanswered question is how this approach will perform in complex propagation environments, where the GPS signal and corresponding positioning quality may be rapidly fluctuating. Furthermore, it is unclear if the computational requirements for this type of approach are compatible with embedded applications.

5.2. GPS Spoofing Detection

GPS spoofing has been a recent topic of intense interest; therefore, there are many published papers on the subject. There are three primary approaches for GPS spoofing detection: ML-based, antenna/direction-of-arrival (DOA)-based, and movement tracking-based (Table 10).

Table 10. Summary of most common approaches in the literature to GPS spoofing detection.

Type of Approach	General Idea	Strengths	Key Open Research Questions
ML-based	Use measurable features of GPS signal, spoofed signal, and GPS receiver to train an ML model for future predictions on future data based on those same features.	Based on easily observable parameters. Demonstrated good performance.	Can ML models be sufficiently optimized to run on small platforms with limited computational capability?
Antenna/DOA-based	Utilize antenna array to measure aspects of signal to discern between authentic signals and spoofed signals.	Based on easily observable parameters, few computational requirements. Demonstrated good performance.	Can antenna arrays be made sufficiently simple to be viable for small platforms?
Movement tracking-based	Use the movement history of the platform to identify anomalies and outliers in position estimates.	Simple to implement, few computational requirements. Demonstrated good performance.	How will these approaches work for complex flight paths?

Most of the proposed methods for GPS spoofing detection are based on machine learning approaches. These approaches share a largely common workflow: (1) conduct a set of experiments for which the outputs are known; (2) measure a set of observable parameters that have been deemed essential; (3) compile those measured values along with the known outputs into a training dataset; (4) train the machine learning model; (5) evaluate the performance of that machine learning model with a separate dataset of measured parameters and known outputs; and (6) compare the outputs predicted by the machine learning model with the known outputs. The key differences between the proposed approaches are (1) features chosen for inclusion in model training, (2) model selection, (3) chosen performance metrics, and (4) achieved performance. Table 11 summarizes some of the proposed ML-based approaches.

Table 11. Summary of select ML-based approaches for GPS spoofing detection.

Authors	Reference	Chosen Features Summary	ML Model	Performance Metrics	Achieved Performance
A. Gasimova et al.	[73]	C/No, Various correlator values, Prompt Quadrature Component, Carrier Doppler, Pseudo-Range (PR), Receiver Time, Time of Week, Carrier Phase Cycles, SVN	Ensemble: Stacking	Accuracy Prob Detection Prob Misdetection Prob False Alarm	>95% >99% ~0.5% ~0.1%
C. Titouna and F. Abdelleselam	[74]	SVN, SNR, PR, Doppler Shift, Current Position, Previous Position, Neighbor Position (Swarm)	Bayesian Network	Precision Recall Area under ROC	>90% >85% 0.962
P. Jiang et al.	[75]	Speed, Direction	Recurrent Neural Network	Detection Rate False Alarm Rate	>85% <6%
S. Zuo et al.	[76]	SVN, PR, Doppler Shift, Carrier Phase Frequency Shift, SNR	Isolated Forest	Accuracy	>95%
M. Manesh et al.	[77]	SVN, Carrier Phase, PR, Doppler Shift, SNR	Neural Network	Accuracy Prob Detection Prob False Alarm	~100% ~100% ~0%
T. Khoei et al.	[78]	SVN, Doppler Shift, PR, Receiver Time, Carrier Phase Shift, Various Correlator values, Prompt In-Phase, Prompt Quadrature, Carrier Doppler, SNR	Ensemble: 10 ML models dynamically selected	Accuracy Prob Detection Prob False Alarm Prob Misdetection Processing Time	99.6% 98.9% 1.56% 1.09% 1.24%
M. Nayfeh et al.	[79]	Position, Time, Altitude, GPS speed, Type of GNSS fix, HDOP, VDOP, GPS Noise, Jamming State, Velocity, Number of Satellites, Heading, Timestamp	Decision Tree	Detection Rate Misdetection Rate False Alarm Rate	92% 13% 4%

Table 11. *Cont.*

Authors	Reference	Chosen Features Summary	ML Model	Performance Metrics	Achieved Performance
G. Aissou et al.	[80]	PRN, DO, C/No, Others (Total of 11 Features)	Decision Tree (XGBoost)	Accuracy Prob Detection Prob Misdetection Prob False Alarm	95.5% 95.4% 4.6% 4.3%
S. Semanjski et al.	[81]	C/No, PR, Carrier Doppler, Others (Total of 11 Features)	SVM	Accuracy Prob Misdetection Prob False Alarm	97.8% 7.6% 1.5%
X. Wie et al.	[82]	Magnetometer X-Axis, Mean GPS Altitude, Mean Latitude (Total of 21 Features)	RF, XGBoost	Accuracy Precision Recall F1	99.69% 98.76–99.07% 99.38–99.69% 99.22%
X. Wie et al.	[83]	Latitude, Longitude, Altitude, Speed (Horizontal and Vertical), Roll, Pitch, Yaw, Roll Rate, Pitch Rate, Yaw Rate, Vertical Acceleration	SVM, KNN, RF, GBDT, DT, MLP, XGBoost	Accuracy Precision Recall Missing Mistake F1	97.70% 98.70% 96.76% 3.24% 1.32% 97.72%

For instance, the authors of [84] proposed an SVM-based approach to GPS spoofing detection, where they looked at the difference between position as derived from GPS and the onboard inertial sensors and then determined if the difference was due to spoofing or inertial errors through an SVM model. The authors of [85] presented a linear regression approach to GPS spoofing detection. In this approach, the UAS flight trajectory prediction model was obtained by fitting the UAS's flight log with the linear regression model. The authors of [86] proposed using fuzzy logic in the signal acquisition process. The proposed approach aligns the value of the acquisition threshold using parameters affecting acquisition performance in the presence of the spoofed GPS signal. The ratio between the correlation levels was then used to distinguish between the actual and spoofed GPS signals. The authors of [87] proposed a game-theoretic approach to GPS spoofing detection for UAS applications. The proposed approach viewed the interactions between a GPS spoofer and UAS operator as a Stackelberg game, showing this approach outperformed other game strategies.

ML-based approaches are the current most popular method; however, a wide variety of existing approaches are not ML-based. These approaches can be classified as: (1) antenna-based approaches; (2) movement history-based approaches; and (3) signal statistics-based approaches. Many other proposed approaches do not easily fit into any generalized category or taxonomy.

The authors of [88] proposed a microstrip patch antenna array-based solution that determines the Direction of Arrival (DOA) of the spoofed GPS signal through a DL-based approach. The DOA of authentic GPS signals is roughly known (upward-facing hemisphere); therefore, signals that are determined to have DOA values outside of that plausible range are deemed spoofed signals. The performance of the proposed approach is a function of three parameters: (1) the SNR of the actual GPS signal, (2) the SNR of the spoofed GPS signal, and (3) the number of antenna array elements. Good performance is achieved with a sufficiently high GPS SNR: greater than -4 dB relative to the spoofed signal. The best performance was observed when the number of antenna array elements was greater than six.

Similarly, the authors of [89] proposed an approach to detecting GPS spoofing by determining the DOA of the spoofed signal. The authors of [89] proposed using a compressed sensing method instead of a DL method to estimate the power and DOA of the incoming signal based on off-grid Bayesian inference. Simulation results demonstrated the ability to accurately estimate DOA towards the GPS spoofer when the power of the received spoofed signal was greater than that of the actual GPS signal and when the DOA of the spoofed signal was different from that of the actual GPS satellites. The authors of [90] proposed using a dual-antenna system to calculate the Doppler Frequency Difference of Arrival (FDOA). The approach is predicated on the consistent, predictable nature of the GPSS downlink signal and the fact the presence of a spoofed GPS signal can be determined by detecting subtle differences in carrier frequency and phase, demonstrating that the proposed approach can discern between the actual and spoofed GPS signals. The advantage of this approach is its computational simplicity, since it requires little memory or processing capability. The disadvantage of this approach is the need for multiple antennas that must stay in the same formation during the observation window, making it unclear how well this approach would perform in the case of platform mobility. Another antenna array-based method was proposed by the authors of [91], in which the antenna array would be used to detect spoofed signals based on phase delay measurements. The primary drawback to these approaches is the need for multiple antennas, which may not be practical for small systems.

Other researchers proposed using approaches based on tracking the UAS movement history for GPS spoofing detection. For example, the authors of [92] proposed a multi-sensor approach that combined the onboard IMU sensor with vision methods using a monocular camera onboard the UAS. The proposed approach would use the camera's video stream and IMU sensor to calculate a velocity vector for the UAS. The video feed would be used to estimate platform velocity, and that information would be used to reset IMU error accumulation. Simultaneously, a velocity vector would be calculated based on GPS alone. Those two velocity vectors would be compared, and spoofing would be declared if they were sufficiently different. This approach was implemented on a DJI Phantom 4 UAS and could be detected within an average of five seconds. The authors of [93] also proposed using IMU sensors to detect GPS spoofing attacks. This approach was implemented by integrating an IMU/GNSS into a Kalman filter that monitors anomalies.

Several papers exist in the literature that analyze various aspects of signal statistics, of both the authentic signal and the spoofed signal, in detecting the presence of a spoofing threat. As an example, the authors of [94] considered the use of Doppler frequency and carrier-to-noise (C/N) density ratio as the primary metrics to discern a spoofed signal from an authentic signal. The authors then used numerous types of ML and analytical models to analyze performance utilizing these metrics, including SVM, KNN, RF, Gradient Boosting Decision Tree (GBDT), DT, and XGBoost. The authors of [94] reported accurate spoofing detection rates of 84.88–95.56%, with KNN providing the best results in terms of accuracy for their datasets. SVM provided nearly as good accuracy, with slightly better true positive rate (TPR) performance.

Many other existing approaches do not cleanly fit into a taxonomy. The authors of [95] proposed an approach to GPS spoofing detection that treats GPS spoofing detection as an outlier detection problem, analyzing the time-series history of the position estimates and identifying outlier values through the Grubbs outlier test. Any outlier is a spoofed position estimation in this approach. The authors of [96] also treated GPS spoofing as an outlier problem. They implemented a navigation filter based on a constant velocity model. This model employed a 3D Kalman filter to identify and remove outlier values, which were presumed to be spoofed locations. The authors of [97] also viewed GPS spoofing detection (in part) as an outlier detection problem, employing a Kullback-Leibler divergence measure to search for anomalies in data. The authors coupled this anomaly detection approach with an entropy-based method for spoofing detection. The outstanding question regarding outlier removal approaches is how they would work in dynamic mobile scenarios that do not have a constant velocity model or where signal fading causes rapid signal power fluctuations, both actual and spoofed GPS signals.

Other proposed approaches utilize ADS-B broadcasts from aircraft and UASs to detect GPS spoofing attacks. Ground sensors monitor ADS-B broadcasts while geolocating the corresponding aircraft. It is assumed that the aircraft is a victim of GPS spoofing if the ADS-B broadcast reflects a different position than its actual position. The authors of [98] claimed that this approach can globally detect GPS spoofing attacks in under two minutes, and they can localize the attacker with an accuracy of 150 m within 15 min of monitoring time. The authors of [99] claimed an average detection accuracy and precision of 81.7%

and 85.3%, respectively, based on real-world air traffic control (ATC) data crowdsourced by the OpenSky Network. A potential limitation of these approaches is that, like GPS, ADS-B broadcasts are unauthenticated and can be spoofed.

The authors of [100] utilized a satellite imagery matching technique to detect GPS spoofing attacks in UAS applications. In this approach, DeepSIM uses the onboard camera to capture images of the terrain below and then compare those to existing satellite-based imagery to determine its position, which can then be compared with the position determined via GPS. A discrepancy between the two is illustrative of GPS spoofing. The authors utilized four different DL models to achieve image matching based on whether satellite imagery or aerial imagery was available for the area, including Distance Threshold, Siamese ResNet, Semi-Siamese Network, and Siamese SqueezeNet. The authors reported a GPS spoofing detection rate of over 95% using this approach. A potential limitation of this type of approach is the ability to capture all possible conditions in the DL training datasets to reflect different light conditions (e.g., night versus day), changes in seasons (e.g., foliage changes), manmade or natural-induced changes to terrain, etc.

6. Countermeasures and Their Comparison

6.1. Countermeasures for GPS Jamming

There are limited options to mitigate the effects of interference once it is detected. Mitigations to GPS interference, either intentional or unintentional, primarily focus on the rejection of the interfering signal, minimizing its effect on the GPS receiver. This interference rejection is achieved primarily through antenna-based approaches, such as antenna nulling, or filtering, such as notch filtering the interference.

6.1.1. Antenna-Based Approaches

These approaches are predicated on antenna arrays that can be electronically steered. A null in the received antenna pattern can be formed once the interference signal has been detected, and the power of the interference is reduced while maintaining the power of the actual GPS signal. Many papers in the literature propose an antenna-based approach to mitigate the effects of GPS jamming. These approaches involved complete solutions that included interference detection methods and countermeasures. The factors that differentiated these various proposals were (1) antenna technology, (2) measured signal attributes used for antenna null formation, (3) speed of adaptation, and (4) resultant performance, such as depth of nulls. Many other papers proposed anti-jam GPS antenna designs but did not propose interference detection methods or antenna adaptation algorithms. These papers typically assume their proposed antenna design can be paired with suitable adaptation algorithms and measurement approaches. Other studies presented antenna adaptation algorithms but did not present either detection methods or actual antenna design. Many antenna-based approaches previously discussed for GPS jamming and spoofing detection also apply to GPS jamming mitigation. Table 12 summarizes some of the antenna-based approaches found in the literature.

Table 12. Summary of antenna-based approaches found in the literature for GPS jamming mitigation.

Author	Reference	Type of Proposed Approach	Antenna Technology	Measured Attributes
S. Ni et al.	[71]	Detection Algorithm Adaptation Algorithm	Generic array	Carrier Phase
N. Rezazadeh et al.	[101]	Antenna Design	Multimode microstrip	N/A
Y. Zheng et al.	[102]	Antenna Design	Planar array with annular ring array elements	N/A

Table 12. *Cont.*

Author	Reference	Type of Proposed Approach	Antenna Technology	Measured Attributes
V. Obi et al.	[103]	Antenna Design	Planar array with dipole array elements	N/A
L. Dan et al.	[104]	Adaptation Algorithm	Generic array	Delay estimation, C/A correlation
M. Jayaweera et al.	[88]	Detection Algorithm Adaptation Algorithm Antenna Design	Microstrip patch	Carrier Phase
B. Hao et al.	[105]	Antenna Design Adaptation Algorithm	Dual-polarized Ellipsoid array	Power, polarization mismatch

The question surrounding antenna-based approaches is whether these designs and techniques can be made sufficiently small and simple enough to be feasible options for small systems. Microstrip antennas may be more attractive for UASs than larger arrays; however, small arrays with dipole antenna elements could be feasible, especially for larger unmanned platforms. None of these techniques are likely feasible for smaller unmanned platforms, such as micro UASs.

6.1.2. Signal Processing Approaches

Several approaches exist in the literature based on reducing/removing unwanted interference through signal processing methods, focusing on some form of notch filtering, some of which are summarized in Table 13.

Table 13. Summary of signal processing-based approaches for GPS jamming mitigation.

Author	Reference	Technical Approach	Jamming Threats Addressed
Y. Chien	[106]	Adaptive Notch Filter (ANF)	CW interference
M. Abbasi et al.	[107]	ANF combined with neural network	CW interference
S. Kim et al.	[108]	Transversal Finite Impulse Response (FIR) Filter	Chirp jamming
S. Arif et al.	[68]	Complex Adaptive Notch Filter (CANF)	CW interference

Other research papers have studied the effects of various hardware components on jamming rejection performance, such as the automatic gain control (AGC) function within the GPS receiver [109], in which they performed frequency domain analysis to isolate the desired GPS signal from the jamming signal. This frequency domain method can effectively capture GPS signals and begin processing when the AGC interference-to-noise ratio is at least 37 dB, corresponding to a GPS SNR of approximately 14 dB. These signal-processing approaches are typically effective against only specific types of jamming waveforms; however, they are relatively lightweight in terms of computational or hardware complexity and are likely feasible across many hardware platforms.

Most proposed techniques primarily address narrowband jammer types, such as CW and narrowband chirp jamming. Limited signal processing-based approaches in the literature address wideband jamming threats. Wideband jamming techniques are generally less effective than narrowband techniques, likely due to the spread spectrum nature of the GSM waveform, suggesting that the lack of wideband methods is not a critical gap; however, studies have indicated that partial-band swept noise can be highly effective in disrupting GPS signal reception. Current literature does not address mitigating this type of jamming.

6.2. Countermeasures for Spoofing

Many antenna-based approaches for jamming mitigation can also be applied for GPS spoofing mitigation. Many of these approaches are predicated on determining the DOA of the interfering signal and then creating a null in the receive antenna pattern in the direction of the hostile attack system. Most of these approaches, particularly those that work on the carrier phase, can also be applied to the spoofing threat. Additional papers in the literature presented antenna-based approaches that optimized their detection and antenna nulling specifically to address GPS spoofing by taking advantage of code-based GPS signal structure features. For example, the authors of [91] looked at carrier phase differences in received signals by taking advantage of C/A code symbol alignment properties between the actual and spoofed GPS signals, reporting an attenuation of unwanted signals of at least 60 dB when the SNR of the spoofed signal was high. Most antenna-based methods discussed for GPS spoofing detection also include mitigation approaches focused on creating antenna nulls in the direction of the GPS spoofer. Most signal processing-based approaches to GPS jamming mitigation do not apply to GPS spoofing mitigation. Most papers that propose signal processing-based jamming mitigation approaches primarily address narrowband unwanted signals and cannot remove the wideband spoofed GPS signal.

The common approach to GPS spoofing mitigation is simple message filtering. GPS spoofing detection methods focus on identifying the presence of the spoofed GPS signal. The assumed mitigation approach is for the system to simply ignore the resulting position once it is detected. This capability is essential since the unmanned system will no longer follow false position estimates and can no longer have its flight path manipulated by the GPS spoofer.

6.3. Countermeasures for GPS-Denied Environment—Alternate Positioning

Researchers have proposed many techniques for positioning and navigation in GPS-denied environments over the past two decades [23]. These different approaches are all predicated upon using measurements from onboard sensors to understand its environment, from which position can be inferred. Different approaches utilize different sensors, while some utilize values from multiple sensors. These proposed approaches generally belong to one of six categories (Figure 5) [110].

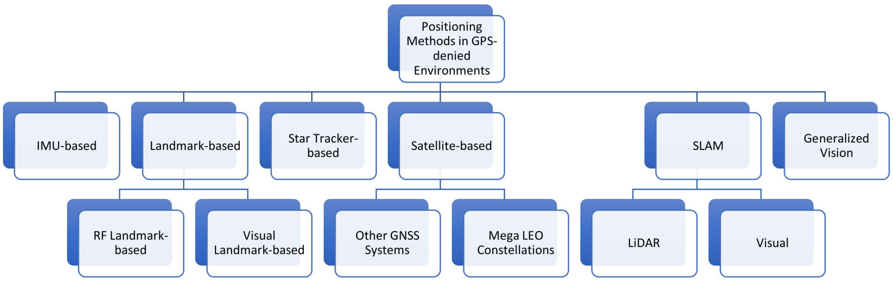


Figure 5. High-Level taxonomy of existing methods for positioning in GPS-denied environments.

Not all systems will possess all sensor types. Consequently, not all alternate positioning methods will universally apply to all unmanned systems. Furthermore, these various approaches have strengths and weaknesses that may make them more applicable to certain use cases. The advantages and disadvantages of these various alternative positioning approaches are summarized in Table 14 [110].

6.3.1. IMU-Based Approaches

IMUs are packaged sensor suites that typically include accelerometers and gyroscopes for each axis of motion and sometimes contain magnetometer sensors. An accelerometer is an instrument that measures linear and angular acceleration, such as changes in speed or direction. Accelerometers can be mechanical, capacitive, or piezoelectric in nature. A gyroscope is a device used to measure or maintain orientation and angular velocity. A magnetometer is a device that measures magnetic field strength, allowing the UAS to always know magnetic north, similar in function to a compass. IMU sensors measure acceleration, orientation, angular rates, and magnetic and gravitational forces. These measurements can then be used to detect and track motion relative to the system's starting point, as in determining relative position and velocity [23]. IMU-based approaches are very mature and can provide highly accurate short-term positioning and navigation results; however, IMU accuracy decreases over time due to inherent error accumulation. These errors can take the form of biases, scale-factor errors, and misalignment errors, leading to significant inaccuracies after as little as one minute of use. IMU calibration procedures can significantly lower these errors; however, some level of error accumulation will generally linger, which will eventually yield inaccurate results. For example, magnetometer sensors often experience noisy measurements due to the strong currents in the electric motor circuits during flight, such as motors turning rotor blades in a quadcopter. Research in the literature provides recommendations for proper ground calibration to minimize this noise [111]. Another common approach is employing extended Kalman filters (EKFs) to dynamically weight IMU sensor measurements, which can further reduce accumulation errors and unwanted biases.

Table 14. Summary of positioning approaches.

Positioning Method	Hardware Requirement	Advantages	Disadvantages	Level of Research Activity
GPS	GPS receiver	• Small lightweight hardware. • Low-cost hardware. • Proven performance.	• Vulnerable to spoofing and jamming attacks. • Poor performance in multipath and shadowing environments.	• Moderate—Some ongoing research on GPS performance.
Receiver-based GPS Performance Improvement	RF hardware (e.g., antenna)	• Demonstrated ability to recover GPS performance in the presence of degradation.	• Additional hardware or computational complexity.	• Moderate—Continuing research in antenna-based and signal processing-based methods for jamming and spoofing suppression/rejection.
IMU	IMU	• Good performance for short flight times. • Successfully used to augment GPS when coverage is intermittent.	• Accuracy decreases over time due to error accumulations.	• High—Stand-alone IMU research is receiving moderate interest. Significant amount of research in multi-sensor IMU methods.
RF Landmark	RF receiver	• High accuracy demonstrated, particularly in dense RF environments. • Proliferation of commercial wireless infrastructure lends itself to wide applicability.	• Some approaches require pre-placed signals along path of movement. • Requires onboard database of known landmark locations. • Performance dependent on environment and geometry.	• Moderate—Various commercial communications infrastructures have been considered in the literature to serve as landmarks.

Table 14. *Cont.*

Positioning Method	Hardware Requirement	Advantages	Disadvantages	Level of Research Activity
Visual Landmark	Camera	• High accuracy has been demonstrated. • Minimal hardware requirements.	• Some approaches require pre-placed physical objects along path of movement. • Requires onboard database of known landmark locations.	• Moderate—Research often coupled with IMU-based methods. This area is more active within the context of Visual SLAM.
Star Tracker	Star tracker	• Good performance in certain conditions.	• Limited utility in daytime or when night sky obscured. • Requires additional star tracker hardware. • Can typically only provide accurate orientation.	• Low—Limited research related to interference suppression and daytime operations.
Alternate GNSS	GNSS receiver	• Low-cost, small hardware, often the same hardware as the GPS receiver.	• Vulnerable to spoofing and DoS attacks. • Poor performance in multipath and shadowing environments.	• Low—Limited research on multi-GNSS performance.
Mega LEO Constellation	RF receiver	• High accuracy has been demonstrated • Mega-constellations less vulnerable to physical attacks.	• Vulnerable to spoofing and DoS attacks. • Additional hardware required. • Many approaches require changes to existing constellations.	• Moderate—Growing research area focused on using commercial LEO constellations for navigation.
LIDAR SLAM	LIDAR transceiver	• Proven performance, has been in use for many years.	• Expensive hardware. • Computationally expensive. • Typical application is regional mapping only.	• Moderate—Mature research area. Perceived decline in research over time. Three-dimensional is more researched than two-dimensional.
Visual SLAM	Camera	• Proven performance, has been in use for many years. • Minimal sensor hardware requirements.	• Computationally expensive. • Typical application is regional mapping only. • Poor performance in low-light.	• High—Significant research in the space of Visual-SLAM. Focus on multi-sensor fusion and IMU-hybrid methods.
Generalized Vision	Camera	• Good performance possible. • Minimal additional hardware requirements.	• Computationally expensive.	• Moderate—Less active research area compared with Visual-SLAM. Much research in the context of hybrid IMU approaches.

Quantum accelerometers are an exciting research area that has the potential to eventually provide very good IMU-based positioning and navigation, primarily due to the extremely low errors these quantum devices produce, meaning that error accumulation would be insignificant; however, quantum accelerometers do not yet exist in a practical form for most applications. Quantum accelerometer technology faces many challenges, making the technology impractical for most platforms. Consequently, researchers are actively searching for methods to improve IMU performance. The authors of [112] have established that the key technical challenges facing quantum accelerometers are (1) a lower sample rate due to cold atom interrogation time and (2) a reduced dynamic range due to signal phase wrapping.

Numerous papers in the literature focus on improving IMU performance for positioning and navigation. Two key trends in the literature propose IMU-based approaches: (1) IMU redundancy and (2) fusion of IMU with other onboard sensors into multi-fusion ensemble approaches.

The authors of [113] proposed an approach that employs an array of six commercial-grade inertial sensors arranged in a cube containing triaxial gyros, accelerometers, and magnetometers. This approach aims to compensate for individual sensor bias using mutual calibration. This mutual calibration is accomplished by calculating average values across all sensors for each spatial axis. This approach was demonstrated in a vehicle-based experimental testbed with reported average position accuracy within 1.1 m. The multi-IMU approach outperformed GPS-based positioning during experimentation, providing an average position accuracy within 3.52 m. The authors of [113] continued their work in [114], focusing on the accuracy of attitude determination in UAS applications. They again used their multi-IMU system with six IMUs in a cubic configuration and focused on assessing the accuracy of roll, pitch, and heading. The reported root mean square error (RMSE) was extremely low, with heading, pitch, and roll errors reported as 0.032, 0.012, and 0.023 radians, respectively. The authors of [115] proposed a multi-IMU redundancy approach, where they fused measurements from five different IMUs using a feedback-federated Kalman filter with attitude estimation using the Bortz equation, resulting in the best performance of all methods considered. This approach achieved very low errors in estimating the test platform's roll, pitch, and yaw compared with ground truth. These various research efforts established the feasibility of using multi-IMU approaches in terms of achievable performance. The major challenge with these approaches is the higher cost and required sensor hardware, which may be prohibitive for some systems.

The research presented in these papers has one primary limitation: they all evaluate their solutions in well-controlled vehicle-based or small UAS-based systems in seemingly benign environments. One main limitation of IMUs is that inertial sensors are extremely sensitive to environmental and platform factors, such as temperature, pressure, mechanical vibration, and electrical system noise, in the case of magnetometers. Many unmanned systems will be expected to operate in harsh environments that may produce fluctuations in these parameters and significant system vibration, which complicates effective IMU calibration. The mutual self-calibration approach proposed in [113] is promising since it may solve this problem; however, additional experiments and analyses are required to determine performance under harsh conditions.

Most IMU-related research focuses on multi-sensor fusion and using additional sensors to improve IMU-based positioning performance. The underlying concept of these approaches is that IMUs can provide very accurate positioning solutions for limited periods of time due to error accumulation. Additional sensors are used to periodically achieve an accurate ground-truth position estimate that can be used to reset the IMU-based method. The IMU-based method then needs to simply maintain accuracy until the next ground-truth solution can be achieved via the other sensors. A common approach is using a hybrid IMU-GNSS approach with GPS-provided ground truth to reset inertial accumulation errors, with the IMU maintaining positioning during GPS intermittent outages. This approach does not work in the GPS-denied environment; another sensor is required to provide this ground-truth IMU reset function.

The authors of [116] proposed an inertial navigation algorithm that incorporates sensor outputs from accelerometers, gyroscopes, magnetometers, Pitot tubes, and air vanes; however, a stated goal of their approach was to facilitate the fusion of their proposed inertial filter with visual odometry methods. Several papers have proposed using magnetometer sensor outputs to improve IMU performance. The authors of [117] proposed to fuse inertial and magnetometer sensors using a Kalman filter to improve performance. The authors of [118] proposed an integration of IMU outputs with magnetometer sensor outputs to improve accuracy in attitude initialization. Numerous papers have proposed fusing IMU-based techniques with various sensors that may be onboard the UAS, including vision techniques utilizing an onboard monocular camera [119], altitude estimation using a range sensor [120], SLAM techniques using LiDAR [121], and LEO satellite tracking [122]. Several research papers also propose a joint IMU-GPS positioning solution to improve performance where GPS reception is intermittent or inaccurate, such as in urban environments [43,123]. These papers report low-achieving position estimation errors, generally within 10 m. The primary disadvantage of these proposed methods is the need to include additional sensors onboard the platform.

Few studies have proposed ML-based approaches for nonlinear processing to minimize inertial drift. For example, the authors of [124] proposed a method where IMU sensor output error would be estimated and corrected by employing a non-linear auto-regressive neural network with exogenous inputs cascaded with a multi-layer perceptron (MLP)-based neural network. The proposed approach outperformed recurrent neural network (RNN)-based and legacy EKF approaches. The authors of [124] reported position estimation accuracy improvements over tactical-grade IMUs of 30%, 44%, and 80% for GPS outages of 10, 25, and 50 s. These results are encouraging; however, error drift still limits the useful timeframe for navigation based on IMUs alone.

Redundant IMU and multi-sensor fusion methods offer good performance with a low cost of computational complexity. The major disadvantage of these approaches is the need for additional sensor hardware onboard the UAS, which may be problematic for small and low-cost systems; however, there are examples of multi-sensor fusion approaches working on small micro-UASs. The authors of [125] demonstrated a multi-sensor fusion navigation system onboard a micro-UAS that utilized 3D LiDAR, a stereo camera, an altimeter, and IMU sensors, with data fused using a synchronization and time delay compensation algorithmic strategy. This research demonstrated that these multi-sensor approaches are achievable on small UAS platforms.

A technical challenge not addressed in the literature is the initial determination of the ground-truth position. IMU-based methods provide relative position information and must have an accurate ground truth from which to start. Onboard sensors may prove less useful in providing this ground truth. This problem may require manual intervention if the unmanned system is initiated from a well-known location.

There have been proposed methods that rely solely on magnetometer sensors for navigation [126]. The MagNav concept uses Earth's magnetic field to uniquely identify any point globally. Good performance has been observed using MagNav approaches, reaching the destination of a 1500-mile flight to within 1 km of accuracy using nothing but a magnetometer and machine learning algorithms trained on magnetic field map data. A significant challenge with this approach is that Earth's magnetic field is constantly changing, requiring periodic magnetic field surveying and model retraining.

6.3.2. Landmark-Based Approaches

Many techniques for positioning and navigation in the literature are based on the idea of detecting known objects within the environment, such as landmarks. These approaches utilize the known position of landmark objects so that the UAS knows its location when that object is encountered. The logic behind this concept can be best explained with this illustration: I know where that thing is located. I see that thing. By extension, I know where I am. We have already seen variations of these approaches in the IMU approach discussions. Other sensors are used to locate recognizable objects in the multi-sensor fusion IMU approach, establishing a ground-truth position estimate that can be used to reset IMU accuracy. The landmark concept is identical, except an IMU is not necessarily present. Instead, position and navigation may be achieved solely through landmark recognition. Landmark recognition may also be used intermittently in conjunction with other sensors, such as an IMU. Landmark-based positioning requires the UAS to maintain knowledge of known object locations so that when that object is encountered, it can be mapped to a location. The "object" can be any phenomenon that can be observed via a UAS sensor. The existing ones commonly fall into one of two categories: (1) RF landmarks and (2) visual landmarks.

RF landmark-based approaches use existing communications infrastructure for position calculation, which could take the form of signal emitters pre-placed along the UAS flight path. This approach requires a priori knowledge of the flight path and the installation of ground-based infrastructure. These types of approaches have been effective in the case of visual landmarks [127] and also perform well in the case of RF landmarks [128]. This pre-placement approach may prove valuable in applications where a UAS always performs a fixed flight path; however, it may not be practical for generalized UAS operations.

A more flexible approach is utilizing existing commercial communications infrastructure for position calculation. In this case, existing commercial signals are viewed as Signals of Opportunity (SOPs) that are received by the UAS platform. The locations of many types of commercial RF emitters are publicly known; therefore, it would be possible to build an onboard emitter location database that could be used to detect SOPs and estimate the receiver's position. There are many papers in the literature where commercial SOPs are used for navigation purposes, including IEEE 802.11-based Wi-Fi [129], Bluetooth [130], AM Radio [131], FM Radio [132,133], Digital Television (DTV) [134], and cellular communications [135]. The authors of [136] implemented an SDR-based system onboard a small quadcopter UAS using FM radio, DTV, cellular, and Wi-Fi SOPs for positioning, demonstrating good position accuracy performance. It is unclear how SOPs such as Wi-Fi and Bluetooth could be incorporated into a generalized positioning system since Wi-Fi and Bluetooth locations are not always publicly known; however, many of the other SOPs, including AM radio, FM radio, DTV, and cellular infrastructure, lend themselves to a generalized approach since their emitter locations are well known and publicly available. Many technical attributes of these emitters, such as transmit power and antenna type, are also publicly available.

One limitation of this approach is that it will not necessarily be applicable across all geographic locations. Many papers in the literature focus on urban and suburban regions; however, there will be a less dense communications infrastructure for many of these signal types, such as DTV, in rural and less populated regions. A promising approach for positioning is using signals from the commercial cellular communications infrastructure as SOPs. Previous studies have revealed that good accuracy can be obtained; however, accuracy depends on the environment, and position accuracy is sensitive to interference [135]. Numerous studies in the literature demonstrate that good position accuracy can be obtained using 4G LTE cellular SOPs [135,137–141]. There is also a growing amount of literature demonstrating that good performance can be obtained using 5G cellular SOPs [142–144]. Previous work has demonstrated accurate positioning using CDMA-based cellular SOPs [145].

Cellular SOPs could be cooperative or uncooperative. A cooperative SOP paradigm means that the system is a participating member of the cellular network. This approach allows the User Equipment (UE) to receive positioning information from the cellular network via its existing positioning method, such as the LTE Positioning Protocol (LPP) in 4G cellular networks. Cellular UE positioning via these built-in positioning methods and the high accuracy of these methods are well understood; however, research has suggested that the performance of these methods may be sensitive to jamming and interference [143]. This approach may not work in regions without significant cellular infrastructure, such as unpopulated desert regions. There are also potential negative impacts on the overall cellular network associated with UAS-based UEs. This issue is due to the increased visibility of the cellular network by the UAS-based UE, potentially increased uplink interference, and a higher number of system handoffs [146]. The second approach is uncooperative in nature, where the system is equipped with an RF receiver capable of passively observing cellular signals and using them as landmarks but is not a valid user of the cellular network.

A fundamental concern with RF-landmark-based approaches is that these signals are all unauthenticated, and while publicly available information is valuable in developing an onboard knowledge base, it is also valuable to someone launching a malicious attack. It is feasible that someone could mount an attack where they not only spoof GPS but also any of the signals mentioned above since SDR technology is easy to obtain due to its convenience and low cost. This aspect of RF-landmark research has not been addressed in the literature to date.

Visual landmark-based approaches are predicated on detecting landmarks in imagery captured via a camera sensor. These landmarks can be either manmade or natural and, combined with some type of onboard knowledge base, could be used to determine position with high demonstrated accuracy [127,147]. An example of landmark preplacement for visual recognition in support of navigation can be found in [148], where landmarks are strategically established in a partially known environment to support robot navigation. Another example can be found in [149], where the authors used a monocular camera onboard a robotic ground vehicle to detect pre-placed landmarks that served as waypoint markers. The generalized applicability of these approaches is limited due to their reliance on well-known existing landmarks or pre-placed objects along the path of movement; however, these approaches may be useful when operating in known areas or fixed flight paths. These types of approaches could also be helpful in hybrid approaches. Combining visual landmark-based approaches with IMU-based approaches can achieve high position estimation accuracy [115], where visual recognition provides intermittent high-accuracy ground-truth position estimates that can be used for IMU accumulation error reset. The authors of [115,127] demonstrated that this type of approach can work well within sufficiently dense regions with visually identifiable landmarks. For example, consider using roads as landmarks, where a UAS equipped with a monocular camera detects roads within images taken from the camera and recognizes the ground road pattern to determine its own position. This approach has been proposed by multiple papers in the literature [150,151], with good position accuracy performance reported; however, landmark-based approaches do not perform well in feature-sparse regions, such as deserts and oceans. Furthermore, many of these approaches rely on ML-based neural network approaches that will place a computational requirement on the UAS.

There are several technical challenges associated with visual landmark-based navigation. These methods are typically computationally expensive and may not be suitable for many unmanned systems; visual methods generally do not perform well in low-light scenarios, which may limit the scenarios in which this method may perform well; and visual methods do not perform well when reference scenery or objects change. Causes of change can be manmade, such as in the presence of construction, or natural, such as changes in seasons or time of day.

6.3.3. Star Tracker-Based Approaches

A star tracker is a sensor that recognizes star patterns in the sky and can be used for navigation purposes. Star tracker-based navigation approaches have existed for thousands of years, particularly in nautical applications. Modern star tracker systems are mature technology. Star tracker systems are commonly used in space-based and aviation-based navigation applications; however, star trackers by themselves do not typically provide position estimates. Rather, they are used to determine orientation and can be used in conjunction with other sensors to determine position. Star tracker methods can achieve high accuracy in orientation determination. These systems perform well in low-light and clear-sky scenarios; however, their performance suffers in daylight hours due to interference from the sun. Performance also suffers in cloudy conditions due to the occlusion of the observable stars.

Researchers have recently attempted to leverage star tracker techniques and improve performance, although this is not an active research area. There are examples of researchers attempting to fuse star tracker data with IMU data in a multi-sensor fusion approach [152,153]. There are also examples of ongoing work to attempt to improve star tracker performance during daytime operations [154,155]. The authors of [155] proposed an approach where they characterized ambient polarized skylight and then fused skylight, starlight, and IMU data through a Kalman filter approach. The authors of [154] focused on characterizing sky background radiation and stellar radiation, which can be used to calibrate and configure the star tracker hardware and software for optimal detection. The results from these papers are promising; however, star tracker performance in the daytime continues to be a significant limitation and an unsolved problem. Star tracker systems are often expensive, limiting their applicability to many unmanned systems. This research area is unlikely to experience near-term technical breakthroughs since active research is limited.

6.3.4. Satellite-Based Approaches

There is a growing amount of research on using other satellite systems to augment GPS-based navigation, of which there are two primary categories of approaches: (1) multi-GNSS approaches and (2) commercial LEO constellation-based approaches, such as mega-constellations. Commercial multi-GNSS chipsets can be configured to receive signals from GPS, GLONASS (Russia), Galileo (European Union), and BeiDou (China). Multi-GNSS chipsets inherently mitigate the threat of attack on any one GNSS, with a limited number of papers in the literature that quantitatively support this claim. The authors of [156,157] conducted analyses and experimentation with multi-GNSS receivers to characterize their performance, establishing that multi-GNSS approaches can outperform any single GNSS system. The authors of [157] analyzed the performance of multi-GNSS receivers in the presence of jamming and established that position accuracy is largely unaffected due to the availability of other GNSS systems, even if a single GNSS signal is made unavailable. The authors of [158,159] proposed methods for automatically selecting which GNSS to use for position estimation based on observed conditions. The authors of [159] proposed a method to treat all GNSS constellations as sub-systems of a single system and then selectively choose which satellites from each constellation would be used for position estimation. These papers all demonstrated high position estimation accuracy, as expected, with errors typically of five meters or less. It is intuitively obvious that a multi-GNSS receiver will generally outperform a dedicated GNSS receiver; however, this approach has one key limitation. Other GNSS systems, such as GPS, are susceptible to jamming and spoofing attacks. Consequently, these systems cannot necessarily be trusted any more than GPS. The diversity of employing multiple GNSS systems will improve system robustness; however, an adversary capable and willing to launch an attack on GPS is likely willing and able to do the same against all the other systems. Developing a multi-GNSS jamming or spoofing attack with the SDR-based attack systems found in the literature would be relatively straightforward.

There is an increasing amount of research in the literature that is focused on the use of non-GNSS satellite systems such as Starlink, OneWeb, OrbComm, and Iridium for navigation [160], with Starlink receiving the most interest in the literature to date. These constellations are extremely large (thousands of satellites) and very fast-moving from the perspective of a ground-based observer due to their Low Earth Orbit (LEO) positions, which largely mitigates a physical attack scenario. Much of the work in the literature has been performed by Kassas and his research team, the authors of [160] and numerous other papers on the subject [161–165]. The authors investigated using numerous features of the downlink signals from these constellations, with a focus on Starlink. Some of the more promising signal characteristics are carrier phase and carrier Doppler shift.

Other research teams have recently begun studying the use of these commercial mega-constellations for navigation purposes [166–169]. Many of the proposed methods would require modification to the downlink signal of these commercial systems, which is unlikely to happen; however, many other proposed approaches are completely passive and utilize the as-is downlink signals. The results presented in these papers are promising and demonstrate that this is a feasible concept; however, the downlink signals from these systems will likely be susceptible to jamming or spoofing attacks, especially given the capability and flexibility of SDR-based GPS attack systems.

6.3.5. SLAM Approaches

Simultaneous Localization and Mapping (SLAM) is a special category of navigation and positioning that aims to characterize and navigate a local GPS-denied environment via its onboard sensors. SLAM methods generally fall into three categories:

(1) Light Detection and Ranging (LIDAR)-based SLAM [170–177];
(2) Visual-SLAM (vSLAM) [178–190];
(3) Hybrid Visual-LiDAR SLAM [191,192].

These SLAM approaches typically consider the scenario of an unmanned vehicle navigating a localized region, such as a small UAS exploring an underground cave system. These approaches can be either map-based, where the UAS is attempting to navigate an area from a known map, or mapless, where the unmanned system is attempting to navigate an area while simultaneously creating a map of the region. In both cases, the unmanned system attempts to detect features in the environment and use those features to determine its location. LiDAR-SLAM approaches detect regional features via LiDAR sensors. A primary limitation of LiDAR is cost, since LiDAR sensors are expensive compared with other sensor types, limiting their applicability. vSLAM approaches use the onboard camera sensor. Most vSLAM techniques propose monocular camera sensors that serve vSLAM or VO purposes [193–195]. A primary limitation of vSLAM is its computational complexity, which also limits its applicability. There is a relatively even mixture of 2D versus 3D LiDAR-SLAM papers in the literature; however, 2D LiDAR-SLAM is far more mature. Most 3D LiDAR-SLAM papers focus on finding solutions to the various challenges of 3D SLAM.

These approaches are mature and have demonstrated their ability to map and navigate highly complex environments, including obstacle avoidance; however, they typically do not provide absolute positioning solutions. SLAM methods may not directly apply to generalized positioning and navigation; however, much of the research within the SLAM community is directly applicable to approaches for generalized positioning. For example, significant research within the vSLAM community is focused on improving object and feature detection performance in low-light conditions, which is also a limitation within the generalized vision approaches to positioning, and lessons learned across these communities will benefit both groups.

6.3.6. Generalized Vision Approaches

vSLAM methods typically operate in specific regions and do not necessarily provide absolute positioning; however, generalized vision-based approaches attempt to provide generalized absolute position estimates. Landmark-based vision approaches attempt to determine position based on simple landmarks; however, generalized vision approaches aim to operate on general terrain imagery to provide absolute positioning, including using latitude and longitude. Consider the case of a UAS-based system, where a UAS-based camera sensor observes the ground and an onboard neural network-based algorithm performs terrain recognition to determine the system's position. The authors of [196] proposed an approach where camera imagery was matched to pre-existing aerial satellite imagery to determine location. Factors such as weather, lighting conditions, and seasonal changes to terrain led to poor performance. A positioning accuracy of 36.4 m was achieved using a contrastive learning approach by implementing a convolutional neural network (CNN)-based Siamese neural network that then compared imagery from the UAS camera to aerial satellite imagery. A similar approach was proposed by the authors of [197], who utilized a CNN trained with a large set of preexisting satellite imagery to predict location based on ground images from the UAS camera. The authors of [197] combated issues such as different lighting conditions, weather, and seasonal changes by building a large training dataset that contained images representative of all these conditions. The authors of [110] proposed using the You Only Look Once (YOLO) object recognition algorithm trained on aerial imagery. The trained YOLO model was then used to evaluate imagery from the onboard camera, demonstrating approximately 50-m position estimation resolution with a limited training dataset size; however, the approach performed poorly in regions sparse in features, such as a desert environment. Another interesting approach was proposed by the authors of [198], who built and trained an ML model with images representing each ground coordinate, like the proposed approach in [197]; however, they built the training dataset using Digital Elevation Map (DEM) images for each corresponding location instead of actual images. The goal was to then perform basic image processing on the image from the camera and then input that image into a CNN model for detection and classification. This approach was more immune to changing light conditions and seasonal changes than traditional image-based approaches.

A key technical challenge with generalized vision approaches is the complexity of training the deep learning algorithms typically associated with these approaches. Consider the analysis of this issue presented in [110], which illustrates the dataset size requirements for a single global training dataset sufficiently representative of all locations on Earth. A globally applicable dataset that can achieve 10-m position accuracy resolution would require a minimum dataset size of approximately 1.5×10^{15} images, assuming a single image representing each latitude and longitude coordinate separated by 10 m. These extremely large image training dataset sizes are problematic due to the corresponding computational requirements for model training. The authors of [110] proposed a region-based visual position estimation method with other sensors providing a coarse position estimation, in this case, an RF-based sensor utilizing cellular infrastructure, to mitigate this computational requirement. The resultant coarse position estimate was used to apply a region-specific visual method for precise position estimation selectively. These region-specific visual algorithms were trained against much smaller training datasets specific to a region, reducing computational complexity.

7. Research Gaps, Challenges, and Future Research Directions

Detecting and mitigating threats to the GPS has recently received significant attention. This paper provides an overview of the environments and attacks in which GPS performance may be degraded or lost. GPS jamming and spoofing attacks are becoming increasingly common, and systems capable of executing these attacks can be readily achieved with low- and no-cost commercial hardware and software components with minimal expertise. The data available in the literature illustrate the commonality of GPS jamming attacks worldwide. Unfortunately, no real-world data were found available for GPS spoofing attacks. A useful measurement campaign would be to establish long-term GPS monitoring sites and pair these sites with some of the advanced GPS spoofing detection approaches found in the literature to determine the frequency of GPS spoofing attacks.

Numerous papers in the literature characterize GPS performance. Some of these papers illustrated the performance challenges of GPS in complex multipath and shadowing propagation environments. Some of these papers illustrated the variability in performance across different commercial GPS receivers; however, most of the experiments presented in these papers were not conducted in a controlled manner or with reported rigor. These papers gave a sense of the challenges and performance variability; however, the experimentation methods in most of these papers unfortunately mean that no definitive quantitative conclusions can be drawn from them. Instead, high-level qualitative trends can be inferred from these papers. There are two useful future research activities in this area: (1) controlled and exhaustive experimentation to develop detailed quantitative models of GPS performance variability across GPS receivers, and (2) controlled experimentation to develop detailed channel models for GPS propagation in complex multipath fading and signal shadowing environments. Furthermore, there is a need for additional research to characterize the performance of GPS receivers in the presence of jamming, such as chirp jamming and partial-band noise jamming.

There are a limited number of papers about GPS jamming detection. Most papers focused on two approaches: (1) antenna-based and (2) signal statistics-based. Many of the antenna approaches are promising, but they require antenna arrays that are too large and complex for UAS platforms. Most of the signal statistics-based approaches make simplistic assumptions regarding the propagation environment, and consequently, it is unclear if many of them would perform well in multipath fading or signal shadowing environments. Recent research has employed advanced ML-based approaches for jamming detection and classification. Only a small number of papers in the literature have proposed this approach; however, the results from this limited amount of work are promising. An important future research area would be to expand upon this work and continue maturing ML-based approaches to GPS jammer detection.

The topic of GPS spoofing detection has been extensively studied. Consequently, there is a large amount of research on this subject. The most common approach for GPS spoofing detection is ML-based, which has demonstrated strong performance. There is always room for improvement in any technical approach; however, this research topic has matured.

Despite the wide range of existing methods and approaches for positioning and navigation in GPS-denied environments, existing methods are either scenario- or environment-specific or have other significant limitations. There are many research opportunities for many of the individual alternate positioning and navigation approaches. Research into self-calibrating multi-IMU approaches is promising, but additional research is required to mature the concept, particularly for harsh environments and platform dynamics. Future research should address the security of using unauthenticated RF landmarks. Research is needed to reduce the computational complexity of visual methods of positioning and navigation. Furthermore, methods to improve the performance of visual methods in low-light and changing environmental conditions should be explored. Star tracker approaches should mature through future research. This research area is relatively dormant, but ongoing research is promising, and we believe it could represent an opportunity to provide a reliable means of navigation for many unmanned systems.

Currently, no existing approaches provide universally good performance with reasonably low complexity. Some promising techniques are emerging; however, those most promising techniques would be susceptible to many of the same threats faced by GPS. We have not yet converged on a mature technical solution to this problem due to the wide range of existing methods and approaches, all of which have strengths. Every existing method and approach work well in some situations but poorly in others; therefore, it is possible that there is no single best solution to this problem and that ensemble solutions will be required. From the literature, it appears that researchers, in general, have come to this realization. Most of the recent research papers focused on multi-sensor fusion approaches, where multiple sensor inputs were used jointly to develop position and navigation solutions. It is expected that this trend will continue. One limitation of the current multi-fusion approaches is that they are almost universally focused on two particular sensor data types and are not expandable or modular to incorporate new sensor types. A key future research area would be the development of a generalized multi-sensor fusion framework that could accommodate any sensor type possibly encountered in a plug-and-play fashion. This envisioned framework could operate with any subset of the total possible sensors without configuration or tailoring, which is vital because every UAS platform will likely have a slightly different hardware configuration with different sensors and processing capabilities. The standard approach to multi-sensor fusion is to input data from multiple orthogonal sensors into a Kalman filter to fuse the data and generate a state estimate of the system. The Kalman filter excels at fusing inputs that contain uncertainty due to noise; however, it struggles when a sensor returns anomalous data. Various sensors and approaches have strengths and weaknesses and may produce data that are not relevant in certain environments and conditions, leading to anomalous data that could negatively harm traditional data fusion approaches. Future multi-sensor fusion methods should consider the relevance of sensor data.

A key trend observed in the literature is that recent research across all aspects of detection and mitigation is adopting ML-based approaches, which is expected since ML-based approaches can yield very good results; however, ML-based approaches can be computationally expensive and may not be well-suited for smaller and low-cost UAS platforms. Research into applying sparse dataset training methods, such as zero-shot detection for visual methods, may prove useful.

Finally, based on the strengths and weaknesses of methods found in existing literature, the community has likely not yet converged on an optimal solution, and we must continue to further explore new detection and mitigation strategies against the threats faced by GPS.

Author Contributions: Conceptualization, J.B.; methodology, J.B. and N.K.; investigation, J.B.; writing—original draft preparation, J.B.; writing—reviewing and editing, J.B., T.G. and N.K.; supervision, N.K.; project administration, N.K.; funding acquisition, N.K. All authors have read and agreed to the published version of the manuscript.

Funding: The authors acknowledge the support of the National Science Foundation (NSF), Award Number 2006674.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Manesh, M.R.; Kaabouch, N. Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions. *Comput. Secur.* **2019**, *85*, 386–401. [CrossRef]
2. Tsao, K.-Y.; Girdler, T.; Vassilakis, V.G. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Netw.* **2022**, *133*, 102894. [CrossRef]
3. Durfey, N.; Sajal, S. A Comprehensive Survey: Cybersecurity Challenges and Futures of Autonomous Drones. In Proceedings of the 2022 Intermountain Engineering, Technology and Computing (IETC), Orem, UT, USA, 13–14 May 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–7.
4. Li, L.; Qu, K.; Lin, K.-Y. A Survey on Attack Resilient of UAV Motion Planning. In Proceedings of the 2020 IEEE 16th International Conference on Control & Automation (ICCA), Singapore, 9–11 October 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 558–563.
5. Pirayesh, H.; Zeng, H. Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 767–809. [CrossRef]
6. Yang, Y. Jamming Meets Antijamming: A Survey of GPS Communication Networks. *Secur. Commun. Netw.* **2022**, *2022*, 1–7. [CrossRef]
7. Zidan, J.; Adegoke, E.I.; Kampert, E.; Birrell, S.A.; Ford, C.R.; Higgins, M.D. GNSS Vulnerabilities and Existing Solutions: A Review of the Literature. *IEEE Access* **2021**, *9*, 153960–153976. [CrossRef]
8. Schmidt, D.; Radke, K.; Camtepe, S.; Foo, E.; Ren, M. A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures. *ACM Comput. Surv.* **2016**, *48*, 1–31. [CrossRef]
9. Psiaki, M.L.; Humphreys, T.E. GNSS Spoofing and Detection. *Proc. IEEE* **2016**, *104*, 1258–1270. [CrossRef]
10. Khan, S.Z.; Mohsin, M.; Iqbal, W. On GPS spoofing of aerial platforms: A review of threats, challenges, methodologies, and future research directions. *PeerJ Comput. Sci.* **2021**, *7*, e507. [CrossRef]
11. Gyagenda, N.; Hatilima, J.V.; Roth, H.; Zhmud, V. A review of GNSS-independent UAV navigation techniques. *Robot. Auton. Syst.* **2022**, *152*, 104069. [CrossRef]
12. Chang, Y.; Cheng, Y.; Manzoor, U.; Murray, J. A review of UAV autonomous navigation in GPS-denied environments. *Robot. Auton. Syst.* **2023**, *170*, 104533. [CrossRef]
13. Couturier, A.; Akhloufi, M.A. A review on absolute visual localization for UAV. *Robot. Auton. Syst.* **2021**, *135*, 103666. [CrossRef]
14. Lu, Y.; Xue, Z.; Xia, G.-S.; Zhang, L. A survey on vision-based UAV navigation. *Geo-Spat. Inf. Sci.* **2018**, *21*, 21–32. [CrossRef]
15. Radmanesh, M.; Kumar, M.; Guentert, H.; Sarim, M. Overview of Path-Planning and Obstacle Avoidance Algorithms for UAVs: A Comparative Study. *Unmanned Syst.* **2018**, *6*, 95–118. [CrossRef]
16. Arafat, M.Y.; Alam, M.M.; Moh, S. Vision-Based Navigation Techniques for Unmanned Aerial Vehicles: Review and Challenges. *Drones* **2023**, *7*, 89. [CrossRef]
17. Wei, W.; Tan, L.; Jin, G.; Lu, L.; Sun, C. A Survey of UAV Visual Navigation Based on Monocular SLAM. In Proceedings of the 2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China, 14–16 December 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1849–1853.

18. Sahili, A.R.; Hassan, S.; Sakhrieh, S.; Mounsef, J.; Maalouf, N.; Arain, B.; Taha, T. A Survey of Visual SLAM Methods. *IEEE Access* **2023**, *11*, 139643–139677. [CrossRef]
19. Chahine, G.; Pradalier, C. Survey of Monocular SLAM Algorithms in Natural Environments. In Proceedings of the 2018 15th Conference on Computer and Robot Vision (CRV), Toronto, ON, Canada, 8–10 May 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 345–352.
20. Gaia, J.; Orosco, E.; Rossomando, F.; Soria, C. Mapping the Landscape of SLAM Research: A Review. *IEEE Lat. Am. Trans.* **2023**, *21*, 1313–1336. [CrossRef]
21. Khan, M.U.; Zaidi, S.A.A.; Ishtiaq, A.; Bukhari, S.U.R.; Samer, S.; Farman, A. A Comparative Survey of LiDAR-SLAM and LiDAR based Sensor Technologies. In Proceedings of the 2021 Mohammad Ali Jinnah University International Conference on Computing (MAJICC), Karachi, Pakistan, 15–17 July 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–8.
22. Zhu, J.; Li, H.; Zhang, T. Camera, LiDAR, and IMU Based Multi-Sensor Fusion SLAM: A Survey. *Tsinghua Sci. Technol.* **2024**, *29*, 415–429. [CrossRef]
23. Balamurugan, G.; Valarmathi, J.; Naidu, V.S. Survey on UAV navigation in GPS denied environments. In Proceedings of the 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, Odisha, India, 3–5 October 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 198–204.
24. Huang, L. Review on LiDAR-based SLAM Techniques. In Proceedings of the 2021 International Conference on Signal Processing and Machine Learning (CONF-SPML), Stanford, CA, USA, 14 November 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 163–168.
25. Lai, D.; Zhang, Y.; Li, C. A Survey of Deep Learning Application in Dynamic Visual SLAM. In Proceedings of the 2020 International Conference on Big Data & Artificial Intelligence & Software Engineering (ICBASE), Bangkok, Thailand, 30 October–1 November 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 279–283.
26. Rezwan, S.; Cho, W.I. Artificial Intelligence Approaches for UAV Navigation: Recent Advances and Future Challenges. *IEEE Access* **2022**, *10*, 26320–26339. [CrossRef]
27. GPS.gov. GPS Interface Specifications. Available online: https://www.gps.gov/technical/icwg/ (accessed on 29 July 2024).
28. Hussain, A.; Magsi, H.; Ahmed, A.; Hussain, H.; Khand, Z.H.; Akhtar, F. The effects of using variable lengths for degraded signal acquisition in GPS receivers. *IJECE* **2021**, *11*, 3201. [CrossRef]
29. Hegarty, C.J. GNSS signals—An overview. In Proceedings of the 2012 IEEE International Frequency Control Symposium Proceedings, Baltimore, MD, USA, 21–24 May 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 1–7.
30. Montenbruck, O.; Steigenberger, P.; Hauschild, A. Comparing the 'Big 4'—A User's View on GNSS Performance. In Proceedings of the 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR, USA, 20–23 April 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 407–418.
31. Pesce, V.; Colagrossi, A.; Silvestrini, S. *Modern Spacecraft Guidance, Navigation, and Control*; Elsevier: Amsterdam, The Netherlands, 2023.
32. Morton, Y.T.J.; Diggelen, F.; Spilker, J.J.; Parkinson, B.W.; Lo, S.; Gao, G. (Eds.) *Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications*, 1st ed.; Wiley: Hoboken, NJ, USA, 2020.
33. GPS Performance Standards & Specifications, GPS.gov. Available online: https://www.gps.gov/technical/ps/2020-SPS-performance-standard.pdf (accessed on 29 July 2024).
34. Engel, U. A theoretical performance analysis of the modernized GPS signals. In Proceedings of the 2008 IEEE/ION Position, Location and Navigation Symposium, Monterey, CA, USA, 5–8 May 2008; IEEE: Piscataway, NJ, USA, 2008; pp. 1067–1078.
35. Rychlicki, M.; Kasprzyk, Z.; Rosiński, A. Analysis of Accuracy and Reliability of Different Types of GPS Receivers. *Sensors* **2020**, *20*, 6498. [CrossRef] [PubMed]
36. De Salas, J.; Torroja, M. Carrier phase positioning experiences in consumer GNSS devices. In Proceedings of the 2016 International Conference on Localization and GNSS (ICL-GNSS), Barcelona, Spain, 28–30 June 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–6.
37. Modsching, M.; Kramer, R. Field trial on GPS Accuracy in a medium size city: The influence of built-up. In Proceedings of the 3rd Workshop on Positioning, Navigation and Communication 2006 (WPNC'06), Hannover, Germany, 16 March 2006.
38. Misra, P.; Burke, B.; Pratt, M.M. GPS performance in navigation. *Proc. IEEE* **1999**, *87*, 65–85. [CrossRef]
39. Conley, R. GPS Performance: What Is Normal? *Navigation* **1993**, *40*, 261–281. [CrossRef]
40. Spilker, J.J. GPS Signal Structure and Performance Characteristics. *Navigation* **1978**, *25*, 121–146. [CrossRef]
41. Skournetou, D.; Lohan, E.-S. Ionospheric delay corrections in multi-frequency receivers: Are three frequencies better than two? In Proceedings of the 2011 International Conference on Localization and GNSS (ICL-GNSS), Tampere, Finland, 29–30 June 2011; IEEE: Piscataway, NJ, USA, 2011; pp. 181–186.
42. Merry, K.; Bettinger, P. Smartphone GPS accuracy study in an urban environment. *PLoS ONE* **2019**, *14*, e0219890. [CrossRef]
43. Chiang, K.-W.; Duong, T.; Liao, J.-K. The Performance Analysis of a Real-Time Integrated INS/GPS Vehicle Navigation System with Abnormal GPS Measurement Elimination. *Sensors* **2013**, *13*, 10599–10622. [CrossRef]
44. Eliardsson, P.; Alexandersson, M.; Pattinson, M.; Hill, S.; Waern, Å.; Ying, Y.; Fryganiotis, D. Results from measuring campaign of electromagnetic interference in GPS L1-band. In Proceedings of the 2017 International Symposium on Electromagnetic Compatibility—EMC EUROPE, Angers, France, 4–7 September 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–6.
45. Mitch, R.H.; Dougherty, R.C.; Psiaki, M.L.; Powell, S.P.; O'Hanlon, B.W.; Bhatti, J.A.; Humphreys, T.E. Signal characteristics of civil GPS jammers. In Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation, Portland, OR, USA, 20–23 September 2011; Volume 2011, pp. 1907–1919.
46. Mitch, R.H.; Dougherty, R.C.; Psiaki, M.L.; Powell, S.P.; O'Hanlon, B.W.; Bhatti, J.A.; Humphreys, T.E. Know Your Enemy: Signal Characteristics of Civil GPS Jammers. *GPS World* **2012**, *23*, 64–71.

47. Steiner, J.; Lukes, P. Wide-Area GPS Interference Over Europe From an Unknown Source. In Proceedings of the 2022 New Trends in Civil Aviation (NTCA), Prague, Czech Republic, 26–27 October 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 51–55.
48. Farlik, J.; Kratky, M.; Casar, J. Detectability and jamming of small UAVs by commercially available low-cost means. In Proceedings of the 2016 International Conference on Communications (COMM), Bucharest, Romania, 9–10 June 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 327–330.
49. Ferreira, R.; Souto, N.; Gaspar, J.; Sebastião, P. Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms. *Wirel. Pers. Commun.* **2020**, *115*, 2705–2727. [CrossRef]
50. Saputro, J.A.; Hartadi, E.E.; Syahral, M. Implementation of GPS Attacks on DJI Phantom 3 Standard Drone as a Security Vulnerability Test. In Proceedings of the 2020 1st International Conference on Information Technology, Advanced Mechanical and Electrical Engineering (ICITAMEE), Yogyakarta, Indonesia, 13–14 October 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 95–100.
51. Karpe, R.V.; Kulkarni, S. Software Defined Radio based Global Positioning System Jamming and Spoofing for Vulnerability Analysis. In Proceedings of the 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2–4 July 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 881–888.
52. Ferreira, R.; Gaspar, J.; Souto, N.; Sebastião, P. Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms. In Proceedings of the 2018 Global Wireless Summit (GWS), Chiang Rai, Thailand, 25–28 November 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 27–32.
53. Elezi, E.; Cankaya, G.; Boyaci, A.; Yarkan, S. The effect of Electronic Jammers on GPS Signals. In Proceedings of the 2019 16th International Multi-Conference on Systems, Signals & Devices (SSD), Istanbul, Turkey, 21–24 March 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 652–656.
54. Tamazin, M.; Karaim, M.; Elghamrawy, H.; Noureldin, A. A Comprehensive Study of the Effects of Linear Chirp Jamming on GNSS Receivers under High-Dynamic Scenarios. In Proceedings of the 2018 13th International Conference on Computer Engineering and Systems (ICCES), Cairo, Egypt, 18–19 December 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 9–14.
55. Hunkeler, U.; Colli-Vignarelli, J.; Dehollain, C. Effectiveness of GPS-jamming and counter-measures. In Proceedings of the 2012 International Conference on Localization and GNSS, Starnberg, Germany, 25–27 June 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 1–4.
56. Ahmad, M.; Farid, M.A.; Ahmed, S.; Saeed, K.; Asharf, M.; Akhtar, U. Impact and Detection of GPS Spoofing and Countermeasures against Spoofing. In Proceedings of the 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 30–31 January 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–8.
57. Kerns, A.J.; Shepard, D.; Bhatti, J.A.; Humphreys, T.E. Unmanned Aircraft Capture and Control Via GPS Spoofing. *J. Field Robot.* **2014**, *31*, 617–636. [CrossRef]
58. Mendes, D.; Ivaki, N.; Madeira, H. Effects of GPS Spoofing on Unmanned Aerial Vehicles. In Proceedings of the 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), Taipei, Taiwan, 4–7 December 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 155–160.
59. Yi, S.; Li, X.; You, L. Research on Improvement of Code Phase Synchronization Accuracy in GPS Spoofing. In Proceedings of the 2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China, 12–14 June 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 385–390.
60. Bethi, S.; Pathipati, A. Stealthy GPS Spoofing: Spoofer Systems, Spoofing Techniques and Strategies. In Proceedings of the 2020 IEEE 17th India Council International Conference (INDICON), New Delhi, India, 10–13 December 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–7.
61. Humphreys, T.E.; Ledvina, B.M.; Psiaki, M.L.; O'Hanlon, B.W.; Kintner, P.M. 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, USA, 16–19 September 2008; pp. 2314–2325.
62. Margana, B.S.; Achanta, D.S.; Songala, K.K.; Ammana, S.R. A Simple SDR based Method to Spoof Low-End GPS aided Drones for Securing Locations. In Proceedings of the 2021 IEEE International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON), Dhaka, Bangladesh, 3–4 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 32–36.
63. Ueki, T.; Yoshii, K.; Shimamoto, S.; Mizuno, K.; Matsufuji, K. Evaluation of Impact of Intermediate GPS Spoofing to Mobile Terminals. In Proceedings of the 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 717–718.
64. Songala, K.K.; Ammana, S.R.; Ramachandruni, H.C.; Achanta, D.S. Simplistic Spoofing of GPS Enabled Smartphone. In Proceedings of the 2020 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE), Bhubaneswar, India, 26–27 December 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 460–463.
65. Guo, Y.; Wu, M.; Tang, K.; Tie, J.; Li, X. Covert Spoofing Algorithm of UAV Based on GPS/INS-Integrated Navigation. *IEEE Trans. Veh. Technol.* **2019**, *68*, 6557–6564. [CrossRef]
66. Demir, M.O.; Kurt, G.K.; Pusane, A.E. On the Limitations of GPS Time-Spoofing Attacks. In Proceedings of the 2020 43rd International Conference on Telecommunications and Signal Processing (TSP), Milan, Italy, 7–9 July 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 313–316.
67. Elezi, E.; Cankaya, G.; Boyaci, A.; Yarkan, S. A detection and identification method based on signal power for different types of Electronic Jamming attacks on GPS signals. In Proceedings of the 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Istanbul, Turkey, 8–11 September 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–5.

68. Arif, S.W.; Coskun, A.; Kale, I. Multi-Stage Complex Notch Filtering for Interference Detection and Mitigation to Improve the Acquisition Performance of GPS. In Proceedings of the 2018 14th Conference on Ph.D. Research in Microelectronics and Electronics (PRIME), Prague, Czech Republic, 2–5 July 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 165–168.
69. Wang, J.; Xiao, Y.; Li, T.; Chen, C.L. A Jamming Aware Artificial Potential Field Method to Counter GPS Jamming for Unmanned Surface Ship Path Planning. *IEEE Syst. J.* **2023**, *17*, 4555–4566. [CrossRef]
70. Sakorn, C.; Supnithi, P.; Phakphisut, W. Jamming Detection and Distance Calculation of L1 and E1 Frequencies. In Proceedings of the 35th International Technical Conference on Circuits/Systems, Computers, and Communications (ITC-CSCC), Nagoya, Japan, 3–6 July 2020.
71. Ni, S.; Cui, J.; Cheng, N.; Liao, Y. Detection and elimination method for deception jamming based on an antenna array. *Int. J. Distrib. Sens. Netw.* **2018**, *14*, 155014771877446. [CrossRef]
72. Alkhatib, M.; McCormick, M.; Williams, L.; Leon, A.; Camerano, L.; Al Shamaileh, K.; Devabhaktuni, V.; Kaabouch, N. Classification and Source Location Indication of Jamming Attacks Targeting UAVs via Multi-output Multiclass Machine Learning Modeling. In Proceedings of the 2024 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 6–8 January 2024; IEEE: Piscataway, NJ, USA, 2024; pp. 1–5.
73. Gasimova, A.; Khoei, T.T.; Kaabouch, N. A Comparative Analysis of the Ensemble Models for Detecting GPS Spoofing attacks on UAVs. In Proceedings of the 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 26–29 January 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 0310–0315.
74. Titouna, C.; Nait-Abdesselam, F. A Lightweight Security Technique For Unmanned Aerial Vehicles Against GPS Spoofing Attack. In Proceedings of the 2021 International Wireless Communications and Mobile Computing (IWCMC), Harbin City, China, 28 June–2 July 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 819–824.
75. Jiang, P.; Wu, H.; Xin, C. DeepPOSE: Detecting GPS spoofing attack via deep recurrent neural network. *Digit. Commun. Netw.* **2022**, *8*, 791–803. [CrossRef]
76. Zuo, S.; Liu, Y.; Zhang, D.; Xin, P.; Liu, T. Detection of GPS Spoofing Attacks Based on Isolation Forest. In Proceedings of the 2021 IEEE 9th International Conference on Information, Communication and Networks (ICICN), Xi'an, China, 25–28 November 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 357–361.
77. Manesh, M.R.; Kenney, J.; Hu, W.C.; Devabhaktuni, V.K.; Kaabouch, N. Detection of GPS Spoofing Attacks on Unmanned Aerial Systems. In Proceedings of the 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 11–14 January 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
78. Khoei, T.T.; Ismail, S.; Kaabouch, N. Dynamic Selection Techniques for Detecting GPS Spoofing Attacks on UAVs. *Sensors* **2022**, *22*, 662. [CrossRef] [PubMed]
79. Nayfeh, M.; Li, Y.; Shamaileh, K.A.; Devabhaktuni, V.; Kaabouch, N. Machine Learning Modeling of GPS Features with Applications to UAV Location Spoofing Detection and Classification. *Comput. Secur.* **2023**, *126*, 103085. [CrossRef]
80. Aissou, G.; Slimane, H.O.; Benouadah, S.; Kaabouch, N. Tree-based Supervised Machine Learning Models For Detecting GPS Spoofing Attacks on UAS. In Proceedings of the 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 1–4 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 0649–0653.
81. Semanjski, S.; Muls, A.; Semanjski, I.; De Wilde, W. Use and Validation of Supervised Machine Learning Approach for Detection of GNSS Signal Spoofing. In Proceedings of the 2019 International Conference on Localization and GNSS (ICL-GNSS), Nuremberg, Germany, 4–6 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
82. Wei, X.; Wang, Y.; Sun, C. PerDet: Machine-Learning-Based UAV GPS Spoofing Detection Using Perception Data. *Remote Sens.* **2022**, *14*, 4925. [CrossRef]
83. Wei, X.; Sun, C.; Lyu, M.; Song, Q.; Li, Y. ConstDet: Control Semantics-Based Detection for GPS Spoofing Attacks on UAVs. *Remote Sens.* **2022**, *14*, 5587. [CrossRef]
84. Panice, G.; Luongo, S.; Gigante, G.; Pascarella, D.; Di Benedetto, C.; Vozella, A.; Pescapè, A. A SVM-based detection approach for GPS spoofing attacks to UAV. In Proceedings of the 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, UK, 7–8 September 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–11.
85. Meng, L.; Yang, L.; Ren, S.; Tang, G.; Zhang, L.; Yang, F.; Yang, W. An Approach of Linear Regression-Based UAV GPS Spoofing Detection. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 1–16. [CrossRef]
86. Tohidi, S.; Mosavi, M.R. Fuzzy-based acquisition in GPS receivers for spoofing mitigation. *Microprocess. Microsyst.* **2023**, *101*, 104886. [CrossRef]
87. Eldosouky, A.; Ferdowsi, A.; Saad, W. Drones in Distress: A Game-Theoretic Countermeasure for Protecting UAVs Against GPS Spoofing. *IEEE Internet Things J.* **2020**, *7*, 2840–2854. [CrossRef]
88. Jayaweera, M. A Novel Deep Learning GPS Anti-spoofing System with DOA Time-series Estimation. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6.
89. Yang, Q.; Chen, Y. A GPS Spoofing Detection Method Based on Compressed Sensing. In Proceedings of the 2022 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), Xi'an, China, 25–27 October 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–5.
90. He, L.; Li, H.; Lu, M. Dual-antenna GNSS spoofing detection method based on Doppler frequency difference of arrival. *GPS Solut.* **2019**, *23*, 78. [CrossRef]

91. Magiera, J.; Katulski, R. Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing. *J. Appl. Res. Technol.* **2015**, *13*, 45–57. [CrossRef]
92. Qiao, Y.; Zhang, Y.; Du, X. A Vision-Based GPS-Spoofing Detection Method for Small UAVs. In Proceedings of the 2017 13th International Conference on Computational Intelligence and Security (CIS), Hong Kong, China, 15–18 December 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 312–316.
93. Tanil, C.; Khanafseh, S.; Joerger, M.; Pervan, B. An INS Monitor to Detect GNSS Spoofers Capable of Tracking Vehicle Position. *IEEE Trans. AerosElectron. Syst.* **2018**, *54*, 131–143. [CrossRef]
94. 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. [CrossRef]
95. Pardhasaradhi, B.; Lingadevaru, P.; Bn, B.R.; Srihari, P.; Cenkeramaddi, L.R. Robust Positioning and Grubbs Outlier Test for Navigation in GPS Spoofing Environment. In Proceedings of the 2022 IEEE 19th India Council International Conference (INDICON), Kochi, India, 24–26 November 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–6.
96. Pardhasaradhi, B.; Srihari, P.; Aparna, P. Navigation in GPS Spoofed Environment Using M-Best Positioning Algorithm and Data Association. *IEEE Access* **2021**, *9*, 51536–51549. [CrossRef]
97. Basan, E.; Basan, A.; Nekrasov, A.; Fidge, C.; Sushkin, N.; Peskova, O. GPS-Spoofing Attack Detection Technology for UAVs Based on Kullback–Leibler Divergence. *Drones* **2021**, *6*, 8. [CrossRef]
98. Jansen, K.; Schafer, M.; Moser, D.; Lenders, V.; Popper, C.; Schmitt, J. Crowd-GPS-Sec: Leveraging Crowdsourcing to Detect and Localize GPS Spoofing Attacks. In Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–24 May 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1018–1031.
99. Liu, G.; Zhang, R.; Wang, C.; Liu, L. Synchronization-Free GPS Spoofing Detection with Crowdsourced Air Traffic Control Data. In Proceedings of the 2019 20th IEEE International Conference on Mobile Data Management (MDM), Hong Kong, China, 10–13 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 260–268.
100. Xue, N.; Niu, L.; Hong, X.; Li, Z.; Hoffaeller, L.; Pöpper, C. DeepSIM: GPS Spoofing Detection on UAVs using Satellite Imagery Matching. In Proceedings of the Annual Computer Security Applications Conference, Austin, TX, USA, 7–11 December 2020; ACM: New York, NY, USA, 2020; pp. 304–319.
101. Rezazadeh, N.; Shafai, L. GPS anti-jamming performance of multimode microstrip antennas. In Proceedings of the 2016 17th International Symposium on Antenna Technology and Applied Electromagnetics (ANTEM), Montreal, QC, Canada, 10–13 July 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–2.
102. Zheng, Y.; Huang, Y.; Wang, Y.E. Design of Small GPS Anti-Jam Antenna. In Proceedings of the 2018 IEEE International Symposium on Antennas and Propagation & USNC/URSI National Radio Science Meeting, Boston, MA, USA, 8–13 July 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1289–1290.
103. Obi, V.; Evans, G.; Lim, S. Design of a Miniaturized, High Gain, Anti-Jam Global Positioning System (GPS) Antenna. In Proceedings of the SoutheastCon 2022, Mobile, AL, USA, 26 March–3 April 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 73–74.
104. Lu, D.; Wu, R.; Wang, W. Robust widenull anti-jamming algorithm for high dynamic GPS. In Proceedings of the 2012 IEEE 11th International Conference on Signal Processing, Beijing, China, 21–25 October 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 378–381.
105. Hao, C.; Liu, Y.; Wang, X.; Sun, X. A Modified Anti-Jamming Method Using Dual-Polarized Ellipsoid Minimum Variance Distortionless Response to Predict the Coverage Ratio of Global Positioning System Signal. *IEEE Sens. J.* **2021**, *21*, 26839–26847. [CrossRef]
106. Chien, Y.-R. Design of GPS Anti-Jamming Systems Using Adaptive Notch Filters. *IEEE Syst. J.* **2015**, *9*, 451–460. [CrossRef]
107. Abbasi, M.; Mosavi, M.R.; Reazei, M.J. GPS Continues Wave Jamming Canceller using an ANF Combined with an Artificial Neural Network. In Proceedings of the 2020 8th Iranian Joint Congress on Fuzzy and intelligent Systems (CFIS), Mashhad, Iran, 2–4 September 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 99–104.
108. Kim, S.; Park, K.; Seo, J. Mitigation of GPS Chirp Jammer Using a Transversal FIR Filter and LMS Algorithm. In Proceedings of the 2019 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), JeJu, Republic of Korea, 23–26 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–4.
109. Zhou, Z.; Wei, Y. The Influence of Automatic Gain Control on Narrowband Frequency Domain GPS Anti-Jamming Receiver. In Proceedings of the 2021 IEEE 21st International Conference on Communication Technology (ICCT), Tianjin, China, 13–16 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 497–501.
110. Burbank, J.; Foust, L.; Greene, T.; Kaabouch, N. A Proposed Framework for UAS Positioning in GPS-Denied and GPS-Spoofed Environments. In Proceedings of the 24th Integrated Communications, Navigation, and Surveillance Conference (ICNS), Herndon, VA, USA, 23–25 April 2024.
111. Pesterev, A.V.; Morozov, Y.V.; Matrosov, I.V.; Ashjaee, J. Estimation of the magnetic field generated by UAV in flight. In Proceedings of the 2018 25th Saint Petersburg International Conference on Integrated Navigation Systems (ICINS), St. Petersburg, Russia, 28–30 May 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–4.
112. Wang, X.; Kealy, A.; Gilliam, C.; Haine, S.; Close, J.; Moran, B.; Talbot, K.; Williams, S.; Hardman, K.; Freier, C.; et al. Enhancing Inertial Navigation Performance via Fusion of Classical and Quantum Accelerometers. *arXiv* **2021**, arXiv:2103.09378.
113. Alteriis, G.D.; Accardo, D.; Moriello, R.S.L.; Ruggiero, R.; Angrisani, L. Redundant configuration of low-cost inertial sensors for advanced navigation of small unmanned aerial systems. In Proceedings of the 2019 IEEE 5th International Workshop on Metrology for AeroSpace (MetroAeroSpace), Torino, Italy, 19–21 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 672–676.

114. De Alteriis, G.; Conte, C.; Moriello, R.S.L.; Accardo, D. Use of Consumer-Grade MEMS Inertial Sensors for Accurate Attitude Determination of Drones. In Proceedings of the 2020 IEEE 7th International Workshop on Metrology for AeroSpace (MetroAeroSpace), Pisa, Italy, 22–24 June 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 534–538.
115. Patel, U.N.; Faruque, I.A. Multi-IMU Based Alternate Navigation Frameworks: Performance & Comparison for UAS. *IEEE Access* **2022**, *10*, 17565–17577.
116. Gallo, E.; Barrientos, A. Reduction of GNSS-Denied inertial navigation errors for fixed wing autonomous unmanned air vehicles. *Aerosp. Sci. Technol.* **2022**, *120*, 107237. [CrossRef]
117. Tkhorenko, M.; Karshakov, E.; Papusha, I. Inertial Navigation Aiding by the Means of Magnetic Measurements. In Proceedings of the 2023 30th Saint Petersburg International Conference on Integrated Navigation Systems (ICINS), Saint Petersburg, Russia, 29–31 May 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1–3.
118. De Alteriis, G.; Bottino, V.; Conte, C.; Rufino, G.; Moriello, R.S.L. Accurate Attitude Inizialization Procedure based on MEMS IMU and Magnetometer Integration. In Proceedings of the 2021 IEEE 8th International Workshop on Metrology for AeroSpace (MetroAeroSpace), Naples, Italy, 23–25 June 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6.
119. Hardy, J.; Strader, J.; Gross, J.N.; Gu, Y.; Keck, M.; Douglas, J.; Taylor, C.N. Unmanned aerial vehicle relative navigation in GPS denied environments. In Proceedings of the 2016 IEEE/ION Position, Location and Navigation Symposium (PLANS), Savannah, GA, USA, 11–14 April 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 344–352.
120. Jao, C.-S.; Wang, Y.; Shkel, A.M. A Zero Velocity Detector for Foot-mounted Inertial Navigation Systems Aided by Downward-facing Range Sensor. In Proceedings of the 2020 IEEE SENSORS, Rotterdam, The Netherlands, 25–28 October 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–4.
121. Ariante, G.; Papa, U.; Ponte, S.; Del Core, G. UAS for positioning and field mapping using LIDAR and IMU sensors data: Kalman filtering and integration. In Proceedings of the 2019 IEEE 5th International Workshop on Metrology for AeroSpace (MetroAeroSpace), Torino, Italy, 19–21 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 522–527.
122. Saroufim, J.; Hayek, S.W.; Kassas, Z.M. Simultaneous LEO Satellite Tracking and Differential LEO-Aided IMU Navigation. In Proceedings of the 2023 IEEE/ION Position, Location and Navigation Symposium (PLANS), Monterey, CA, USA, 24–27 April 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 179–188.
123. Khosyi'in, M.; Budisusila, E.N.; Prasetyowati, S.A.D.; Suprapto, B.Y.; Nawawi, Z. Design of Autonomous Vehicle Navigation Using GNSS Based on Pixhawk 2.1. In Proceedings of the 2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Semarang, Indonesia, 20–21 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 175–180.
124. El Sabbagh, M.S.; Maher, A.; Abozied, M.A.H.; Kamel, A.M. Promoting navigation system efficiency during GPS outage via cascaded neural networks: A novel AI based approach. *Mechatronics* **2023**, *94*, 103026. [CrossRef]
125. Lu, H.; Shen, H.; Tian, B.; Zhang, X.; Yang, Z.; Zong, Q. Flight in GPS-denied environment: Autonomous navigation system for micro-aerial vehicle. *Aerosp. Sci. Technol.* **2022**, *124*, 107521. [CrossRef]
126. Bergeron, L.; Nielsen, A. Aeromagnetic Anomaly Mapping for Navigation. In Proceedings of the 2023 IEEE/ION Position, Location and Navigation Symposium (PLANS), Monterey, CA, USA, 24–27 April 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 821–828.
127. Sundar, K.; Srinivasan, S.; Misra, S.; Rathinam, S.; Sharma, R. Landmark Placement for Localization in a GPS-denied Environment. In Proceedings of the 2018 Annual American Control Conference (ACC), Milwaukee, WI, USA, 27–29 June 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 2769–2775.
128. Wang, Z.; Liu, R.; Liu, Q.; Han, L.; Thompson, J.S. Feasibility Study of UAV-Assisted Anti-Jamming Positioning. *IEEE Trans. Veh. Technol.* **2021**, *70*, 7718–7733. [CrossRef]
129. Ying, J.; Pahlavan, K. Precision of RSS-Based Localization in the IoT. *Int. J. Wirel. Inf. Netw.* **2019**, *26*, 10–23. [CrossRef]
130. Ariante, G.; Ponte, S.; Del Core, G. Bluetooth Low Energy based Technology for Small UAS Indoor Positioning. In Proceedings of the 2022 IEEE 9th International Workshop on Metrology for AeroSpace (MetroAeroSpace), Pisa, Italy, 27–29 June 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 113–118.
131. McEllroy, J.; Raquet, J.; Temple, M. Use of a software radio to evaluate signals of opportunity for navigation. In Proceedings of the 2006 19th International Technical Meeting of the Satellite Division of The Institute of Navigation, Fort Worth, TX, USA, 26–29 September 2006; pp. 126–133.
132. Chen, X.; Wei, Q.; Wang, F.; Jun, Z.; Wu, S.; Men, A. Super-Resolution Time of Arrival Estimation for a Symbiotic FM Radio Data System. *IEEE Trans. Broadcast.* **2020**, *66*, 847–856. [CrossRef]
133. Psiaki, M.L.; Slosman, B.D. Tracking Digital FM OFDM Signals for the Determination of Navigation Observables. *NAVIGATION J. Inst. Navig.* **2022**, *69*, navi.521. [CrossRef]
134. Yang, C.; Soloviev, A. Mobile Positioning with Signals of Opportunity in Urban and Urban Canyon Environments. In Proceedings of the 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR, USA, 20–23 April 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1043–1059.
135. Kim, E.; Shin, Y. Feasibility Analysis of LTE-Based UAS Navigation in Deep Urban Areas and DSRC Augmentation. *Sensors* **2019**, *19*, 4192. [CrossRef] [PubMed]
136. Souli, N.; Kolios, P.; Ellinas, G. Online Relative Positioning of Autonomous Vehicles Using Signals of Opportunity. *IEEE Trans. Intell. Veh.* **2022**, *7*, 873–885. [CrossRef]

137. Zhu, H.; Xu, W.; Sang, Y.; Yao, Z.; Liu, L.; Okonkw, M.C. Mobile Communication Signal Selection Algorithm for Signal of Opportunity Navigation. In Proceedings of the 2022 24th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Republic of Korea, 7–10 February 2021; IEEE: Piscataway, NJ, USA, 2022; pp. 166–171.
138. Shamaei, K.; Khalife, J.; Kassas, Z.M. Exploiting LTE Signals for Navigation: Theory to Implementation. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 2173–2189. [CrossRef]
139. Dun, H.; Tiberius, C.C.J.M.; Janssen, G.J.M. Positioning in a Multipath Channel Using OFDM Signals With Carrier Phase Tracking. *IEEE Access* **2020**, *8*, 13011–13028. [CrossRef]
140. Khalife, J.; Kassas, Z.M. On the Achievability of Submeter-Accurate UAV Navigation With Cellular Signals Exploiting Loose Network Synchronization. *IEEE Trans. AerosElectron. Syst.* **2022**, *58*, 4261–4278. [CrossRef]
141. Khalife, J.; Kassas, Z.M. Differential Framework for Submeter-Accurate Vehicular Navigation With Cellular Signals. *IEEE Trans. Intell. Veh.* **2023**, *8*, 732–744. [CrossRef]
142. Gante, J.; Sousa, L.; Falcao, G. Dethroning GPS: Low-Power Accurate 5G Positioning Systems Using Machine Learning. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2020**, *10*, 240–252. [CrossRef]
143. Dwivedi, S.; Shreevastav, R.; Munier, F.; Nygren, J.; Siomina, I.; Lyazidi, Y.; Shrestha, D.; Lindmark, G.; Ernstrom, P.; Stare, E.; et al. Positioning in 5G Networks. *IEEE Commun. Mag.* **2021**, *59*, 38–44. [CrossRef]
144. Abdallah, A.A.; Kassas, Z.M. Opportunistic Navigation Using Sub-6 GHz 5G Downlink Signals: A Case Study on A Ground Vehicle. In Proceedings of the 2022 16th European Conference on Antennas and Propagation (EuCAP), Madrid, Spain, 27 March–1 April 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–5.
145. Khalife, J.; Kassas, Z.M. Navigation With Cellular CDMA Signals—Part II: Performance Analysis and Experimental Results. *IEEE Trans. Signal Process.* **2018**, *66*, 2204–2218. [CrossRef]
146. Muruganathan, S.D.; Lin, X.; Maattanen, H.-L.; Sedin, J.; Zou, Z.; Hapsari, W.A.; Yasukawa, S. An Overview of 3GPP Release-15 Study on Enhanced LTE Support for Connected Drones. *IEEE Comm. Stand. Mag.* **2021**, *5*, 140–146. [CrossRef]
147. Badshah, A.; Islam, N.; Shahzad, D.; Jan, B.; Farman, H.; Khan, M.; Jeon, G.; Ahmad, A. Vehicle navigation in GPS denied environment for smart cities using vision sensors. *Comput. Environ. Urban Syst.* **2019**, *77*, 101281. [CrossRef]
148. Prasad, A.; Sharma, B.; Kumar, S.A. Strategic Creation and Placement of Landmarks for Robot Navigation in a Partially-known Environment. In Proceedings of the 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), Gold Coast, Australia, 16–18 December 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–6.
149. Rebert, M.; Schmitt, G.; Monnin, D. Tracking Visual Landmarks of Opportunity as Rally Points for Unmanned Ground Vehicles. In Proceedings of the 2022 Sixth IEEE International Conference on Robotic Computing (IRC), Naples, Italy, 5–7 December 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 257–260.
150. Wang, T.; Zhao, Y.; Wang, J.; Somani, A.K.; Sun, C. Attention-Based Road Registration for GPS-Denied UAS Navigation. *IEEE Trans. Neural Netw. Learn. Syst.* **2021**, *32*, 1788–1800. [CrossRef] [PubMed]
151. Zhao, Y.; Wang, T. A Lightweight Neural Network Framework for Cross-Domain Road Matching. In Proceedings of the 2019 Chinese Automation Congress (CAC), Hangzhou, China, 22–24 November 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 2973–2978.
152. Ni, Y.; Dai, D.; Tan, W.; Wang, X.; Qin, S. Installation Error Calibration Method of Stellar/inertial Integrated Navigation System for Star Tracker with Narrow Field of View. In Proceedings of the 2023 30th Saint Petersburg International Conference on Integrated Navigation Systems (ICINS), Saint Petersburg, Russia, 29–31 May 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1–4.
153. Dai, D.; Tan, W.; Wu, W.; Wang, X.; Qin, S. An Optimal Tightly-coupled Stellar/inertial Integrated Navigation Method for Daytime Application. In Proceedings of the 2018 DGON Inertial Sensors and Systems (ISS), Braunschweig, Germany, 11–12 September 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–14.
154. Hailong, Z.; Liang, B.; Zhang, T.; Junpeng, H. Designing considerations for airborne star tracker during daytime. In Proceedings of the 27th Chinese Control and Decision Conference (2015 CCDC), Qingdao, China, 23–25 May 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 4279–4283.
155. Zhang, Q.; Yang, J.; Liu, X.; Guo, L. A Bio-Inspired Navigation Strategy Fused Polarized Skylight and Starlight for Unmanned Aerial Vehicles. *IEEE Access* **2020**, *8*, 83177–83188. [CrossRef]
156. Ferrara, N.G.; Nurmi, J.; Lohan, E.S. Multi-GNSS analysis based on full constellations simulated data. In Proceedings of the 2016 International Conference on Localization and GNSS (ICL-GNSS), Barcelona, Spain, 28–30 June 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–6.
157. Elmasry, O.; Tamazin, M.; Elghamarawy, H.; Karaim, M.; Noureldin, A.; Khedr, M. Examining the benefits of multi-GNSS constellation for the positioning of high dynamics air platforms under jamming conditions. In Proceedings of the 2018 11th International Symposium on Mechatronics and its Applications (ISMA), Sharjah, United Arab Emirates, 4–6 March 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.
158. Park, K.W.; Seo, B.-S.; Suh, J.-W.; Park, C. A Method of Channel Selection for Multi-GNSS Receiver. In Proceedings of the 2019 International Conference on Electronics, Information, and Communication (ICEIC), Auckland, New Zealand, 22–25 January 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–3.
159. Soininen, T.; Syrjärinne, P.; Ali-Loytty, S.; Schmid, C. Data-Driven Approach to Satellite Selection in Multi-Constellation GNSS Receivers. In Proceedings of the 2018 8th International Conference on Localization and GNSS (ICL-GNSS), Guimaraes, Portugal, 26–28 June 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.
160. Kassas, Z.M.; Kozhaya, S.; Kanj, H.; Saroufim, J.; Hayek, S.W.; Neinavaie, M.; Khairallah, N.; Khalife, J. Navigation with Multi-Constellation LEO Satellite Signals of Opportunity: Starlink, OneWeb, Orbcomm, and Iridium. In Proceedings of the 2023

IEEE/ION Position, Location and Navigation Symposium (PLANS), Monterey, CA, USA, 24–27 April 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 338–343.

161. Khalife, J.; Neinavaie, M.; Kassas, Z.Z. The First Carrier Phase Tracking and Positioning Results With Starlink LEO Satellite Signals. *IEEE Trans. AerosElectron. Syst.* **2022**, *58*, 1487–1491. [CrossRef]
162. Kassas, Z.M. Navigation from Low-Earth Orbit: Part 2: Models, Implementation, and Performance. In *Position, Navigation, and Timing Technologies in the 21st Century*, 1st ed.; Morton, Y.T.J., Diggelen, F., Spilker, J.J., Parkinson, B.W., Lo, S., Gao, G., Eds.; Wiley: Hoboken, NJ, USA, 2020; pp. 1381–1412.
163. Khalife, J.; Kassas, Z.Z.M. Performance-Driven Design of Carrier Phase Differential Navigation Frameworks With Megaconstellation LEO Satellites. *IEEE Trans. AerosElectron. Syst.* **2023**, *59*, 2947–2966. [CrossRef]
164. Kozhaya, S.E.; Kassas, Z.M. Positioning with Starlink LEO Satellites: A Blind Doppler Spectral Approach. In Proceedings of the 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring), Florence, Italy, 20–23 June 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1–5.
165. Neinavaie, M.; Kassas, Z.M. Signal Mode Transition Detection in Starlink LEO Satellite Downlink Signals. In Proceedings of the 2023 IEEE/ION Position, Location and Navigation Symposium (PLANS), Monterey, CA, USA, 24–27 April 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 360–364.
166. Reid, T.G.; Walter, T.; Enge, P.K.; Lawrence, D.; Cobb, H.S.; Gutt, G.; O'Connor, M.; Whelan, D. Navigation from Low Earth Orbit: Part 1: Concept, Current Capability, and Future Promise. In *Position, Navigation, and Timing Technologies in the 21st Century*, 1st ed.; Morton, Y.T.J., Diggelen, F., Spilker, J.J., Parkinson, B.W., Lo, S., Gao, G., Eds.; Wiley: Hoboken, NJ, USA, 2020; pp. 1359–1379.
167. Iannucci, A.; Humphreys, T.E. Economical Fused LEO GNSS. In Proceedings of the 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR, USA, 20–23 April 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 426–443.
168. Neinavaie, M.; Khalife, J.; Kassas, Z.M. Exploiting Starlink Signals for Navigation: First Results. In Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021), St. Louis, MO, USA, 20–24 September 2021; pp. 2766–2773.
169. Stock, W.; Hofmann, C.A. KnoLEO-PNT With Starlink: Development of a Burst Detection Algorithm Based on Signal Measurements. In Proceedings of the 26th International ITG Workshop on Smart Antennas and 13th Conference on Systems, Communications, and Coding, Braunschweig, Germany, 27–27 February 2023.
170. Shiguang, W.; Chengdong, W. An improved FastSLAM2.0 algorithm using Kullback-Leibler Divergence. In Proceedings of the 2017 4th International Conference on Systems and Informatics (ICSAI), Hangzhou, China, 11–13 November 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 225–228.
171. Li, Z.; Wang, N. DMLO: Deep Matching LiDAR Odometry. In Proceedings of the 2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Las Vegas, NV, USA, 24 October–24 January 2021; IEEE: Piscataway, NJ, USA, 2020; pp. 6010–6017.
172. Paz, L.M.; Jensfelt, P.; Tardos, J.D.; Neira, J. EKF SLAM updates in O(n) with Divide and Conquer SLAM. In Proceedings of the 2007 IEEE International Conference on Robotics and Automation, Rome, Italy, 10–14 April 2007; IEEE: Piscataway, NJ, USA, 2007; pp. 1657–1663.
173. Zhang, J.; Singh, S. LOAM: Lidar Odometry and Mapping in Real-time. In *Robotics: Science and Systems X*; Robotics: Science and Systems Foundation: Berkeley, CA, USA, 2014.
174. Shan, T.; Englot, B. LeGO-LOAM: Lightweight and Ground-Optimized Lidar Odometry and Mapping on Variable Terrain. In Proceedings of the 2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Madrid, Italy, 1–5 October 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 4758–4765.
175. Shan, T.; Englot, B.; Meyers, D.; Wang, W.; Ratti, C.; Rus, D. LIO-SAM: Tightly-coupled Lidar Inertial Odometry via Smoothing and Mapping. In Proceedings of the 2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Las Vegas, NV, USA, 24 October–24 January 2021; IEEE: Piscataway, NJ, USA, 2020; pp. 5135–5142.
176. Zhang, Q.; Zheng, S.; Li, R.; Wang, X.; He, Y.; Wang, X. RLS-LCD: An Efficient Loop Closure Detection for Rotary-LiDAR Scans. *IEEE Sens. J.* **2024**, *24*, 4807–4820. [CrossRef]
177. Huang, Y.; Shan, T.; Chen, F.; Englot, B. DiSCo-SLAM: Distributed Scan Context-Enabled Multi-Robot LiDAR SLAM With Two-Stage Global-Local Graph Optimization. *IEEE Robot. Autom. Lett.* **2022**, *7*, 1150–1157. [CrossRef]
178. Maity, S.; Saha, A.; Bhowmick, B. Edge SLAM: Edge Points Based Monocular Visual SLAM. In Proceedings of the 2017 IEEE International Conference on Computer Vision Workshops (ICCVW), Venice, Italy, 22–29 October 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 2408–2417.
179. Feng, L.; Qu, X.; Ye, X.; Wang, K.; Li, X. Fast Feature Matching in Visual-Inertial SLAM. In Proceedings of the 2022 17th International Conference on Control, Automation, Robotics and Vision (ICARCV), Singapore, 11–13 December 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 500–504.
180. Song, B.; Chen, W.; Wang, J.; Wang, H. Long-Term Visual Inertial SLAM based on Time Series Map Prediction. In Proceedings of the 2019 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Macau, China, 3–8 November 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 5364–5369.
181. Mur-Artal, R.; Montiel, J.M.M.; Tardos, J.D. ORB-SLAM: A Versatile and Accurate Monocular SLAM System. *IEEE Trans. Robot.* **2015**, *31*, 1147–1163. [CrossRef]
182. Wu, X.; Miao, Y.; Sun, Z. ORB-YOLO: An Indoor IMU-aided Visual-Inertial SLAM System for Dynamic Environment. In Proceedings of the 2023 International Conference on Artificial Intelligence of Things and Systems (AIoTSys), Xi'an, China, 19–22 October 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 71–78.

183. Chase, T.; Ali, A.J.B.; Ko, S.Y.; Dantu, K. PRE-SLAM: Persistence Reasoning in Edge-assisted Visual SLAM. In Proceedings of the 2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS), Denver, CO, USA, 19–23 October 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 458–466.
184. Akhloufi, M.A.; Couturier, A. Relative visual localization (RVL) for UAV navigation. In *Degraded Environments: Sensing, Processing, and Display 2018*; Sanders-Reed, J.J.N., Arthur, J.T.J., Eds.; SPIE: Orlando, FL, USA, 2018; p. 28.
185. Jeon, H.; Han, C.; You, D.; Oh, J. RGB-D Visual SLAM Algorithm Using Scene Flow and Conditional Random Field in Dynamic Environments. In Proceedings of the 2022 22nd International Conference on Control, Automation and Systems (ICCAS), Jeju, Republic of Korea, 27 November–1 December 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 129–134.
186. Ruckert, D.; Stamminger, M. Snake-SLAM: Efficient Global Visual Inertial SLAM using Decoupled Nonlinear Optimization. In Proceedings of the 2021 International Conference on Unmanned Aircraft Systems (ICUAS), Athens, Greece, 15–18 June 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 219–228.
187. Couturier, A.; Akhloufi, M.A. UAV navigation in GPS-denied environment using particle filtered RVL. In *Situation Awareness in Degraded Environments 2019*; Sanders-Reed, J.J.N., Arthur, J.T.J., Eds.; SPIE: Baltimore, MD, USA, 2019; p. 24.
188. Gaouti, Y.E.; Khenfri, F.; Mcharek, M.; Larouci, C. Using object detection for a robust monocular SLAM in dynamic environments. In Proceedings of the 2023 IEEE 32nd International Symposium on Industrial Electronics (ISIE), Helsinki, Finland, 19–21 June 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1–6.
189. Yang, S.; Xu, A.; Chen, M.; Shao, K. Visual SLAM Algorithm Based on YOLOv5 in Dynamic Scenario. In Proceedings of the 2023 China Automation Congress (CAC), Chongqing, China, 17–19 November 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 2640–2645.
190. Wang, H.; Sun, Q.; Zou, J.; Liu, W. Visual-Inertial SLAM Algorithm for Low-Texture Subterranean Environments. In Proceedings of the 2023 International Conference on Microwave and Millimeter Wave Technology (ICMMT), Qingdao, China, 14–17 May 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1–3.
191. Anwar, S.; Zhao, Q.; Qadeer, N.; Khan, S.I. A framework for RF-Visual SLAM. In Proceedings of the 2013 10th International Bhurban Conference on Applied Sciences & Technology (IBCAST), Islamabad, Pakistan, 15–19 January 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 103–108.
192. Zhang, J.; Singh, S. Visual-lidar odometry and mapping: Low-drift, robust, and fast. In Proceedings of the 2015 IEEE International Conference on Robotics and Automation (ICRA), Seattle, WA, USA, 26–30 May 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 2174–2181.
193. Volle, G.K.; Willis, A.R.; Brink, K.M. Three Flavors of RGB-D Visual Odometry: Analysis of cost function compromises and covariance estimation accuracy. In Proceedings of the 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR, USA, 20–23 April 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1587–1595.
194. Agarwal, A.; Crouse, J.R.; Johnson, E.N. Evaluation of a Commercially Available Autonomous Visual Inertial Odometry Solution for Indoor Navigation. In Proceedings of the 2020 International Conference on Unmanned Aircraft Systems (ICUAS), Athens, Greece, 1–4 September 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 372–381.
195. Forster, C.; Pizzoli, M.; Scaramuzza, D. SVO: Fast semi-direct monocular visual odometry. In Proceedings of the 2014 IEEE International Conference on Robotics and Automation (ICRA), Hong Kong, China, 31 May–7 June 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 15–22.
196. Ahn, S.; Kang, H.; Lee, J. Aerial-Satellite Image Matching Framework for UAV Absolute Visual Localization using Contrastive Learning. In Proceedings of the 2021 21st International Conference on Control, Automation and Systems (ICCAS), Jeju, Republic of Korea, 12–15 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 143–146.
197. Goforth, H.; Lucey, S. GPS-Denied UAV Localization using Pre-existing Satellite Imagery. In Proceedings of the 2019 International Conference on Robotics and Automation (ICRA), Montreal, QC, Canada, 20–24 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 2974–2980.
198. Wang, T.; Somani, A.K. Aerial-DEM Geolocalization for GPS-denied UAS Navigation. *Mach. Vis. Appl.* **2020**, *31*, 3. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.