Survey of Detection Techniques for GPS Spoofing in Connected Vehicles: Taxonomy, Evaluation, and Future Research Directions

Jing He
School of Media and Exhibition/Modern Intelligent Collaborative Innovation Center for Event Industry Services, Fujian Business University, Fuzhou, 350012, Fujian,China
E-mail: jing_he2@163.com

Keywords: connected vehicles, global positioning system spoofing, detection mechanisms, navigation security

Received: June 1, 2025

The Global Positioning System (GPS) plays a pivotal role in modern vehicular systems by providing accurate navigation and timing services. However, its unencrypted and weak signal structure makes it vulnerable to spoofing attacks, especially in connected vehicle environments. This survey comprehensively reviews GPS spoofing detection techniques, categorizing them into five main approaches: signal processing, machine learning (ML), anomaly detection, cryptographic techniques, and sensor fusion. For each category, we analyze the methods' underlying principles, datasets used (e.g., GNSS-SDR, USRP, simulation-based testbeds), and performance metrics including accuracy, precision, recall, and F1 score. The comparative evaluation highlights that hybrid methods and sensor fusion approaches generally offer higher robustness, while ML-based methods achieve high accuracy but require extensive training data. The paper also identifies key challenges, such as a lack of benchmarking standards and performance variability across dynamic environments. Future directions are proposed to address these limitations and improve the reliability and scalability of GPS spoofing detection systems in real-world connected vehicle applications.

Povzetek: Pregled povzema metode za zaznavanje GPS spoofinga v povezanih vozilih ter izpostavi, da so hibridni in fuzijski pristopi najbolj robustni, a manjkajo standardi za primerjavo.

1 Introduction

Advances in communication and transportation technologies have spurred a diverse range of applications that enhance daily life. These advancements encompass robots, virtual reality, and artificial intelligence, transforming how individuals gain information, interact, and travel [1]. Rapid and cost-effective advancement of the high-speed Internet has prompted the development of new services and applications [2] [3]. With the advent of new wireless technologies, new services and applications such as Self-Organized Networks (SONs) and the Internet of Things (IoT) [4], Wireless Sensor Networks (WSN) [5], Vehicular Ad hoc Networks ($VANET$) [6] , and Mobile Ad hoc Network (MANET) [7] has been made possible. GPS technology has been widely adopted across a vast spectrum of applications—spanning military, commercial, and civilian uses—making it an essential tool in modern life. It is also becoming the main timing system and an essential tool for active microwave remote sensing. In addition, GPS is the primary geodetic tool used to monitor crustal deformation in the geophysics community [8].

Smartphones, mobile devices, cars, and Unmanned Aerial Vehicles (UAVs) are equipped with compact GPS receivers for various functions. These services include proposing routes based on predefined requirements, handling an emergency, and providing location-based services. Therefore, to provide consumers with high-quality services, it is imperative to guarantee GPS availability and dependability [9]. GPS spoofing attacks present serious challenges in the context of connected vehicles, as accurate and dependable GPS signals are important for navigation, positioning, and timing [10]. These types of attacks consist of the use of GPS signals by malevolent users to mislead connected vehicles and misdirect their navigation systems [11]. Through broadcasting fake GPS signals that have high power or accurate timing, attackers can provide fabricated location information that leads to incorrect route directions, incorrect estimation of distances, or even collisions [12]. The significance of strong detection tools for GPS spoofing attacks cannot be underestimated. GPS spoofing attack detection and prevention are important to the integrity and security of GPS signals in connected vehicles. Connected vehicles may unknowingly use fabricated or spoofed GPS information without a good detection system in place, which jeopardizes their safety and might result in serious outcomes [13].

To enhance the detection of GPS systems' spoofing attempts, it is important to incorporate various technologies. The accuracy and comprehensiveness in the detection process are enhanced by the IoT capacity to bridge GPS-capable devices and gather real-time information [14] [15]. The capacity of meta-heuristic algorithms to effectively solve complex optimization problems enables GPS spoofing detection algorithms to perform better [16]. Deep learning (DL) and machine learning (ML) allow systems to learn and adapt, making them capable of differentiating genuine from spoofed GPS signals [17] [18]. Microwave plasma sources play a vital role in the process in that they assist in propagating a controlled environment for the testing and validation of GPS receivers' spoofing resistance [19]. By exposing GPS receivers to spoofing simulation processes, their weaknesses are effectively identified and remedied. Furthermore, urban transportation systems that heavily depend on GPS systems are critical areas for the implementation of a strong spoofing detection mechanism [20]. The vulnerability of public transportation systems to GPS spoofing poses a direct threat to safety and efficiency, necessitating the development of robust detection methods. Therefore, a holistic security approach is indispensable for protecting both the integrity of GPS signals and the safety of all users within today's interconnected vehicular environment. GPS spoofing attack detection also comes with a series of challenging tasks. For example, since fake GPS signals impersonate real GPS signals very well, it is hard for connected vehicles to differentiate between the two. Attackers constantly adapt their techniques, employing sophisticated methods to bypass existing detection systems [6] Another factor to consider is the widespread use of connected vehicles, so successful spoofing attacks can significantly impact multiple vehicles immediately [9]. To effectively tackle these challenges, it is crucial to develop robust detection mechanisms. These systems have to make use of sophisticated signal processing methods, ML algorithms, and anomaly detection strategies to detect and distinguish between real and fake GPS signals precisely. Collaboration between vehicle manufacturers, GPS service providers, and cybersecurity experts is essential [21]. It is possible to improve the detection and mitigation of GPS spoofing attacks by exchanging threat intelligence, developing standardized protocols, and sharing knowledge. For connected cars to remain safe and trustworthy, GPS signals must be secured. Addressing GPS spoofing challenges and implementing robust detection measures will strengthen the resilience of connected vehicles [22] In the context of VANETs, various critical considerations such as QoS and Scalability have been explored to enhance network performance. The security and integrity of GPS data, which are essential for guaranteeing the safe navigation and positioning of connected vehicles, are the main focus of this research, which is unique. This paper presents a comprehensive review of the problems and solutions of GPS spoofing detection in connected vehicles to determine hurdles and outline future directions for research.

In the case of networked vehicles, the increasing security threats posed by GPS spoofing attacks are the motivating force for this endeavor. GPS-based automotive systems have experienced revolutionary advancements as a result of the increasing use of GPS technology in the automotive sector to enhance timing, location, and navigation for both personal and commercial vehicles. Despite the advancements in GPS-based automotive systems, the essentially insecure nature of GPS makes it vulnerable to fraudulent manipulation. With commercial GPS receivers using unencrypted signals that are easily replicable by attackers and the long-distance nature of the transmission of these signals, the vulnerability to GPS spoofing attacks becomes a major problem. In the attack, fake GPS data is inserted into legitimate measurements to falsify vehicles' trajectories and compromise the safety of drivers and pedestrians. The effects of the attack range from incorrect directions to life-threatening collisions, emphasizing the need to create reliable detection mechanisms. The lack of extensive and structured studies in the field of GPS spoofing detection for networked vehicles was the stimulus for this work. Although existing literature discusses various aspects of security in vehicular networks, no holistic analysis of GPS spoofing detection has been conducted. As connected vehicles start to form a part of the transportation system, the reliability and availability of GPS signals are the utmost priority. The present study aims to bridge the gap in the existing research and deliver to the readers a detailed review of current detection approaches, classification of the techniques, as well as a map of the gaps in the areas of research and the directions to proceed. It not only identifies the importance of GPS signal security in connected vehicles but also delivers a strong motivation to the researchers to explore the important area and propose creative solutions to secure the future of the connected vehicular system. In particular, this paper makes the following unique contributions:

- In-depth analysis: The literature is thoroughly reviewed, providing insights into the latest developments and cutting-edge methods in GPS spoofing detection.
- Categorization and comparison: Various detection techniques are categorized and compared, offering a clear framework for understanding the strengths and limitations of each approach.
- This study compares the effectiveness of several GPS spoofing detection techniques using important performance indicators such as Ac, Pr, recall, and $F1$ score. This comparative study sheds important light on the best practices for thwarting GPS spoofing attacks in linked automobiles. By assessing these metrics across different detection techniques, the strengths and weaknesses of each approach are highlighted, aiding in the selection of the most effective strategies.
- Research gaps and future directions: Critical research gaps in GPS spoofing detection for connected vehicles are identified. Highlighting these gaps encourages further exploration and resolution of these challenges in future research.

This is the structure for the remainder of the article. Research methodology is described in Section 2. Section 3 reviews the existing GPS spoofing detection strategies. Section 4 outlines the research gaps and problems, while Section 5 presents the findings.

2 Related works

The study [23] conducts a systematic literature review (SLR) of GPS spoofing attacks, focusing on UAV and GNSS contexts. It categorizes spoofing methods, tools, tests, and techniques, and thoroughly analyzes how various attacks are implemented and detected. The authors also survey existing countermeasures and critically highlight challenges such as the need for real-world validation, the high cost of implementing defenses, and the increasing complexity of attacks and detection algorithms. Their findings provide a structured taxonomy of spoofing strategies and defenses. However, as a survey, it does not introduce new experimental results, and its emphasis on UAVs may limit direct applicability to connected ground vehicles. Its conclusions call for more empirical studies and standardized testing frameworks, aligning with our gap of insufficient real-world validation and benchmarking in spoofing detection.

The work in [24] Presents a comprehensive review of cyberattacks targeting sensors and perception systems in autonomous vehicles. It surveys threats to GPS, LiDAR, cameras, IMUs, and related components, and summarizes machine learning-based defensive techniques. Methodologically, it is a broad narrative review that classifies attacks (including GPS jamming and spoofing) and discusses potential ML defenses to mitigate them. The review highlights how GPS data manipulation can mislead vehicle navigation and underscores general vulnerabilities in autonomy platforms. However, it does not include empirical experiments or propose integrated detection architectures. Its limitations include a lack of new evaluation metrics or real-world testing scenarios; it remains largely descriptive. Thus, while providing useful context on sensor-based attacks, it does not fully address dynamic driving environments or real-time detection frameworks. This gap reinforces the need for practical, validated detection systems that our study aims to explore.

Khan et al. [5] Propose a federated learning (FL) approach for GPS spoofing detection in autonomous vehicles. Using the CARLA driving simulator, each vehicle performs self-localization with onboard sensors (yaw rate, steering angle, wheel speed) and collects both authentic and spoofed trajectories. Local models compute weights from these coordinates, which are then sent to a roadside unit to train a global SVM classifier. FL enables collaborative learning without sharing raw data. The authors report excellent performance (99% accuracy, 98% F1-score) compared to KNN/RF baselines, demonstrating that federated SVM can effectively flag spoofed signals in simulation. However, their method is validated only on simulated CARLA data, not real-world vehicles, and assumes reliable vehicle-to-RSU communication and similar vehicle models. Thus, the approach may not fully capture dynamic traffic conditions or real-world noise, and its practicality under diverse scenarios is untested. This highlights the research gap of limited real-world validation and motivates our work to include live traffic and sensor diversity.

Authors in [13] introduce GPS-IDS, an anomaly-based intrusion detection system for GPS spoofing on autonomous vehicles. The core idea is a physics-based vehicle behavior model: they integrate a GPS navigation model into the conventional dynamic bicycle model to characterize normal AV motion. Temporal features from this model feed into machine learning classifiers that flag deviations as spoofing. They also created the AV-GPS-Dataset (with both real testbed data and CARLA simulations) for evaluation. Results show strong detection: F1 up to 94.4% on real data (with 56.5% faster detection time than a typical EKF-based approach) and 97.1% on simulated urban data. By including real-world experiments, this study directly addresses the validation gap. Its limitations include the controlled nature of the experiments (single vehicle platform, fixed scenarios) and model assumptions (the bicycle model). The generalizability to different vehicle types, multi-vehicle scenarios, or rapidly changing environments is not demonstrated. Such constraints underscore the remaining gap in handling highly dynamic, multi-sensor settings, justifying our focus on broader conditions.

Ying et al. [25] Target GPS spoofing in Connected Vehicle Intersection Movement Assist (IMA) systems. The authors first design an optimization-based attack model that generates realistic spoofed trajectories aimed at triggering false IMA warnings. To defend, they train a one-class classifier (neural network) using only normal vehicle trajectories, enabling detection of unknown spoofing attempts. Using a real-world roundabout dataset, their attack succeeds quickly (<1.7s to trigger IMA), but the detector still identifies anomalies *before* the attack completes. Online detection finds attacks on average 0.49s early, with very low false positive/negative rates. This approach excels in a specific intersection scenario, demonstrating that even aggressive spoofing can be caught. However, it is narrowly scoped: it assumes a fixed roundabout layout and only GPS data, without multi-sensor fusion or adaptation to other road situations. It also relies on offline feature extraction and regular traffic patterns. Its drawbacks include limited generality and no testing under varied traffic or vehicles. These constraints (especially the focus on one scenario) highlight the need for more versatile, scalable detection frameworks, motivating our broader study.

Table 1: Summary of methodology, findings, and limitations of recent GPS spoofing detection studies.

Ref	Methodology	Findings	Limitations
Allão et al. [23]	Systematic literature review of GPS spoofing (UAV focus).	Provides taxonomy of spoofing techniques and defenses; highlights critical needs (e.g., real-world validation).	UAV-centric and survey-only; no new experiments or multi-sensor evaluation; high-level findings with no new data.

Islam et al. [24]	Broad survey of AV sensor and perception attacks (incl. GPS).	Covers numerous attack types and ML-based defenses across sensors; contextualizes GPS spoofing threat.	Descriptive review; lacks empirical analysis or integrated detector design; no real-world benchmarks.
Khan et al.[5]	Federated learning with SVM on CARLA-simulated AV trajectories.	High accuracy (99%) in detecting spoofed trajectories; preserves data privacy by collaborative learning; uses a realistic driving simulator.	Simulation-only (CARLA) experiments; assumes ideal communications and vehicle models; not tested on real traffic.
Abrar et al. [13]	Anomaly detection via physics-based bicycle model (GPS-IDS); new real+sim dataset.	Achieves F1≈94.4% on real data (with faster detection than EKF) and ≈97.1% on simulation; provides first real-world GPS spoofing dataset.	Controlled testbed (single vehicle); may not generalize to other dynamics or multi-vehicle scenarios; relies on model accuracy.
Ying et al. [25]	Optimization-based spoofing attack + one-class neural classifier for IMA.	Can trigger false IMA warning rapidly (<1.7s) and detect it ~0.5s early with very low error; uses only normal data for training.	Focused on one intersection scenario (roundabout); no sensor fusion; assumes consistent traffic behavior; not validated on varied environments.

The reviewed literature, as summarized in Table 1, shows clear advancements in GPS spoofing detection through the use of machine learning, anomaly detection, and federated techniques. High detection accuracies have been reported across several simulated and limited real-world datasets. Review papers contextualize the threat landscape and help establish a taxonomy of countermeasures. However, a consistent limitation across both surveys and empirical studies is the lack of broad real-world validation, diversity in driving environments, and standardized benchmarking protocols. Most existing methods are either scenario-specific, simulation-bound, or assume ideal operating conditions. These gaps, highlighted in both the textual analysis and the comparative evaluation in Table 1, directly motivate the present study, which aims to propose and evaluate a GPS spoofing detection framework designed for scalability, real-time performance, and deployment under varied connected vehicle conditions.

3 Research methodology

This study employed a structured and systematic literature review approach to investigate the current landscape of GPS spoofing detection methods in connected vehicles. To ensure a comprehensive and high-quality synthesis of the relevant research, multiple academic databases were searched, including IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, Wiley Online Library, and Google Scholar. The selection of these databases was based on their relevance and coverage of peer-reviewed publications in the fields of vehicular networks, cybersecurity, and signal processing.

The literature search was conducted using a carefully constructed set of keywords and logical combinations to capture the breadth of research on the subject. These included terms such as “GPS spoofing detection,” “connected vehicles,” “GNSS spoofing mitigation,” “signal processing for GPS spoofing,” “machine learning GPS spoofing,” “sensor fusion GPS security,” and “cryptographic GPS authentication.” The search was restricted to articles published between 2015 and 2024, written in English, and directly related to the detection of GPS spoofing in the context of connected or autonomous vehicles.

To ensure the relevance and quality of the included studies, a set of inclusion and exclusion criteria was applied. Studies were included if they were peer-reviewed journal or conference papers that specifically addressed GPS spoofing detection and employed empirical evaluations, such as simulations or real-world experiments, to report performance metrics, including accuracy, precision, recall, or F1 score. Articles were excluded if they focused solely on GPS jamming rather than spoofing, lacked empirical results, were not published in English, or were duplicates or incomplete in reporting.

After the initial identification and screening process, 78 articles were selected for in-depth analysis. These studies were categorized based on the primary detection approach they employed. Specifically, 17 studies focused on signal processing-based methods, 21 on machine learning techniques, 13 on anomaly detection strategies, 11 on cryptographic solutions, and 16 on sensor fusion-based methods. This categorization enabled a structured evaluation and comparison of the different technological approaches used in combating GPS spoofing.

From each selected study, key information was systematically extracted, including the study's objectives, detection techniques, spoofing scenarios addressed, types of datasets or testbeds used (such as GNSS-SDR and USRP), and performance evaluation methods. The extracted data were synthesized both quantitatively and qualitatively. Quantitative findings were organized into comparative tables (Tables 7 to 11), which presented performance metrics across different methods. Qualitative synthesis involved thematic analysis to identify recurring patterns, emerging trends, and research gaps.

While early drafts described this synthesis as a “meta-analysis,” it is important to clarify that the approach does not involve formal statistical pooling of effect sizes or heterogeneity analysis. Rather, the results presented constitute a descriptive and comparative review of reported outcomes across diverse experimental setups. This methodology offers valuable insights into the state of research in this domain, highlighting the strengths and limitations of various detection techniques and informing future work aimed at enhancing the resilience of GPS systems in connected vehicle environments.

4 GPS spoofing attacks: overview and significance

The GPS has ushered in revolutionary opportunities in a range of industries through better navigation, location-based services, and many applications. There exists a very serious concern due to the inherent security vulnerabilities of GPS technology, particularly when referring to connected cars. Outside the realm of connected vehicles, GPS spoofing attacks pose a very real and dynamic threat to the integrity of GPS signals. GPS spoofing attacks include the injection of spoofed GPS data in authentic GPS measurements to provide falsified trajectories and compromise the safety of road users. GPS spoofing has the potential to affect a range of outcomes from rendering incorrect directions to perpetrating potentially devastating accidents. The need to create efficient detection and prevention systems for GPS spoofing cannot be missed. GPS spoofing attacks are marked by their adaptability and versatility through a range of techniques and approaches that represent a real threat to the integrity of GPS signals. Attackers targeting GPS receivers use a variety of methods that challenge the authenticity of the location as well as the timing information received through these receivers.

- Signal retransmission: Signal retransmission is a very common GPS spoofing attack method. In this attack tactic, attackers receive authorized GPS signals and retransmit them, but slightly change them. These changes are made in a way that skews the data received, resulting in incorrect positioning and navigation information. By replicating genuine GPS signals in a slightly changed form, the attackers have the ability to spoof the receiver's perception of its location, which culminates in incorrect directions or even serious safety risks. Signal retransmission poses a significant threat in applications where accurate navigation is critical, for example, in aviation, sea navigation, or autonomous vehicles.
- Signal replay: Another attack technique used by attackers is signal replay. It involves recording real GPS signals in a given location and then replaying the same signals in the future or at some other geographic location. The attackers aim to trick GPS receivers into thinking that these recorded signals are real and up to date. In this way, attackers might mislead GPS receivers to present inaccuracies in location and navigation. For instance, an attacker might first record the GPS signals close to a secure building and later replay the signals close to the building's gate, which might mislead security systems or facilitate unauthorized entry.
- Signal generation: Alternatively, attackers may use the more advanced and more complicated method of signal generation. This method entails creating entirely synthetic GPS signals, often referred to as spoofed signals. These spoofed signals are designed to mimic authentic GPS signals closely. By generating counterfeit signals that imitate the characteristics of genuine ones, attackers can manipulate GPS receivers into accepting and relying on the false location and timing data provided. Signal generation is particularly concerning because it introduces synthetic signals into the GPS ecosystem, potentially leading to multiple receivers unknowingly relying on manipulated data, with serious consequences for navigation and safety.

5 GPS spoofing detection solutions

In order to trick receivers and mislead users, an attacker can modify GPS signals, as seen in Figure 2. The attacker wants to trick unwary users into relying on fictitious position information by manipulating the GPS signals they receive. Specific geographical areas, such as busy intersections or transportation hubs, are targeted to maximize the impact of the deception. By emitting counterfeit GPS signals using specialized equipment, the attacker creates signals that closely resemble genuine ones, tricking GPS receivers into interpreting them as authentic location information. As a result, users unknowingly follow incorrect routes, posing risks such as collisions or individuals getting lost. The spoofed GPS signals can also disrupt other systems reliant on accurate GPS positioning, like autonomous vehicles or emergency services. Detecting GPS spoofing attacks is challenging due to the similarity between genuine and counterfeit signals, necessitating advanced techniques and specialized equipment for differentiation.

In the preceding section, various GPS spoofing detection techniques were identified. As shown in Figure 3, these techniques can be classified based on underlying principles, including signal processing approaches, ML algorithms, anomaly detection methods, cryptographic techniques, and sensor fusion methods. Each category has its strengths and limitations. Signal processing approaches offer real-time detection capabilities but may be vulnerable to sophisticated spoofing techniques. ML algorithms provide high accuracy but require extensive training data [26]. Anomaly detection methods effectively detect unknown attacks but may produce false positives. Cryptographic techniques enhance signal integrity but may have higher computational requirements. Sensor fusion methods improve detection robustness but may necessitate additional sensor hardware.

5.1 Signal processing approaches

By examining the properties of received GPS signals, several methods are available for identifying GPS spoofing assaults. These methods detect spoofing by monitoring signal strength, time of arrival, and signal consistency. A GPS spoofing detection system depends on the processing of signals for the identification of real as opposed to spoofed signals using the inherent nature of GPS signals. A comparison of the received signals with the expected behavior reveals the spoofing attack. By analysis of the GPS signals received, these algorithms are capable of detecting spoofing efforts and isolating these as opposed to real signals [27]. Signal processing techniques for GPS spoofing detection utilize the following techniques.

- **Signal strength analysis:** Signal strength analysis: It primarily serves to monitor how strong the GPS signals are emanating from satellites. Many spoofing attacks consist of the spoofing of the signal strength so as to deceive the receiver. Discrepancies that signify possible spoofing activity are found through the analysis of discrepancies in the signal strength.
- **Time of Arrival (TOA) Analysis:** GPS signals hold accurate timing data, and spoofing attacks may add delay or modifications to the TOA. Comparing the expected TOA to the observed TOA derived from the received signals using signal processing algorithms depends on the positions of the satellites. Any discrepancy in the expected TOA may signify a spoofing attack.
- **Signal consistency analysis:** GPS signals have consistent patterns in carrier frequency and phase characteristics of the code. Attacks of spoofing will break these patterns, causing irregularity and inconsistency. These irregularities and inconsistencies in patterns are detected by the algorithms for the processing of signals.
- **Multipath analysis:** Multipath results when GPS signals arrive at the receiver along multiple paths, including a direct path and reflected signals. Multipath properties of signals can be spoofed in spoofing attacks. Signal processing algorithms detect spoofing by examining the profiles of the multipath. They detect the anomalies due to spoofing in the multipath profiles.
- **Doppler shift analysis:** Doppler shift occurs as the receiver moves relative to the satellite. Discrepancies in the observed Doppler shift are caused by spoofing attacks. Such discrepancies are identified and marked as possible spoofing events through the use of signal processing algorithms.

Signal processing techniques encompass several algorithms, including cross-correlation, power spectral analysis, statistical analysis, time-frequency analysis, and analysis of the signal-to-noise ratio. These algorithms are contrasted in Table 2 in terms of their strengths and weaknesses. Phase shift and delay caused by a spoofing attack can be detected using cross-correlation-based techniques. Spoofing can be detected by examining temporal anomalies in signals that have already been received. Noise and the interference due to multipath, however, affect the accuracy of cross-correlation computations and render these approaches vulnerable.

In addition to these, there might also be limitations in restraining more advanced spoofing tactics that emulate authentic signal properties. Power spectrum analysis will detect outlying power patterns in GPS signals due to a spoofing attack. It will pick up significant variations in signal properties, including power spikes or plunges. However, the power spectrum analysis might lack the ability to safeguard against advanced spoofing tactics that emulate the power pattern of authentic signals.

Statistical analysis techniques are able to detect changes in statistical patterns in authentic GPS signals. They are capable of observing anomalous signaling behavior that results in spoofing attacks through the examination of diverse statistical parameters. These techniques are vulnerable to changes in the characteristics of the signals due to external conditions and authorized modifications of the signaling. Time-frequency analysis techniques have the ability to view the dynamics and evolution of signals in terms of their changes in time. These techniques have the potential to detect temporal anomalies due to spoofing attacks.

However, it may not always be easy to select the right parameters for the analysis of time-frequency. Time-frequency analysis also has its limitations in the case of intricate changes in a signal. Signal-to-noise ratio analysis examines the extent to which the signals are received. The difference in the quality of signals may help detect counterfeits. An accurate estimation of the noise levels and the signal characteristics is required to analyze signal-to-noise ratios. It may be susceptible to variations in environmental conditions and noise sources.

In general, signal processing techniques offer insightful information about the properties and actions of GPS signals, making it easier to identify GPS spoofing attempts. Nonetheless, the particulars of the spoofing methods and the required detection precision should be taken into account while selecting a method. Combining different strategies and utilizing complementary methodologies might increase the efficacy of GPS spoofing detection systems. To improve the overall accuracy and resilience of GPS spoofing detection systems, signal processing technologies are frequently integrated with other techniques and provide real-time detection capabilities. Nevertheless, sophisticated spoofing techniques can mimic genuine signals, making their detection more challenging. To fully identify GPS spoofing in connected automobiles, it is crucial to combine signal processing techniques with other techniques like ML and anomaly detection.

5.2 Machine learning approaches

ML algorithms have become powerful tools for detecting GPS spoofing by analyzing large amounts of data and recognizing intricate patterns. By identifying the optimal separation lines, Support Vector Machines (SVMs), which are frequently used for binary classification, have shown they are successful at differentiating between real and fake GPS signals. SVMs excel at finding the most discriminating features that enable the accurate classification of GPS signals. Their ability to handle complex data patterns makes them an essential component of GPS spoofing detection systems, particularly in scenarios where the boundary between authentic and spoofed signals is not easily discernible [28] [29]. On the other hand, random forests perform well in noisy and complex environments, avoiding overfitting and excelling at detecting spoofing attacks. They also provide rankings for the importance of different features, helping identify key indicators of spoofing. Given their capacity to extract pertinent information from unprocessed sensor data and understand intricate correlations, neural networks have become more popular in the field of GPS spoofing detection. They do, however, need a significant quantity of labeled training data to function at their best and appropriate regularization to avoid overfitting [30] [31].

When dealing with huge datasets, the straightforward and easy-to-understand K-Nearest Neighbors (KNN) The approach may become computationally costly. GPS signal properties may be modeled, and anomalies can be found using Gaussian Mixture Models (GMM), which are well-known for their capacity to represent intricate data distributions. However, estimating model parameters can be challenging, and GMM may struggle with high-dimensional data or non-Gaussian distributions [32]. The mentioned algorithms are compared in Table 3. ML algorithms perform well in detecting GPS spoofing, but their accuracy cannot be guaranteed. There are three factors to consider when choosing an algorithm: the application's specific needs, the training data available, and the trade-offs that are desired in performance. The strengths and weaknesses of these algorithms can be combined to develop robust and precise GPS spoofing detection systems. For applications such as connected vehicles, these systems are crucial for maintaining GPS signal integrity and security.

5.3 Anomaly detection approaches

Anomalies in GPS data are detected using anomaly detection techniques. These techniques utilize statistical models or algorithms to determine the patterns of GPS signals and detect discrepancies in these patterns. Anomalies are often discovered using unsupervised approaches like One-Class SVM, GMM, and clustering using K-means. Anomaly detection techniques for GPS spoofing detection detect anomalous patterns or activities in GPS signals that represent spoofing. These techniques use statistical analysis, pattern identification, or data mining to recognize discrepancies in the expected properties of genuine GPS signals. The ability of anomaly detection algorithms to detect slight discrepancies in the properties of GPS signals, even as spoofing techniques improve, is one of their primary strengths. Through the examination of statistical properties of GPS signals, these techniques are able to detect discrepancies that might not be easily detectable by human eyes. Table 4 summarizes anomaly detection techniques for the detection of GPS spoofing.

Clustering algorithms, or a form of anomaly detection technique, amalgamate GPS signals according to their similarities in nature. This method has the advantage of being able to detect clusters of GPS signals that have similar patterns, which may indicate spoofing attacks. Clustering algorithms, however, could have trouble identifying sophisticated and dynamic spoofing strategies. This is because they rely on predefined clusters and may not adapt well to new or unknown attack patterns. On the other hand, pattern recognition methods are another category of anomaly detection techniques. These techniques are intended to detect known patterns or spoofing signatures associated with GPS spoofing. They depend on a complete and updated database of known attack patterns to compare the received GPS signals to these known attack patterns. Pattern recognition techniques can identify known spoofing patterns. Because their performance depends on database quality and availability of existing attack signatures, they might have a hard time identifying new or previously unknown attack patterns. Hybrid techniques that incorporate several techniques, including statistical analysis, pattern recognition, and ML, are robust in GPS Spoofing detection. The precision and robustness of GPS Spoofing systems can be enhanced through the use of hybrid techniques that harness the strengths of different detection techniques while suppressing their weaknesses. However, developing and tuning hybrid techniques might need extra computational power and skills.

5.4 Cryptographic approaches

Cryptography-based techniques are very effective in the detection of GPS spoofing in connected vehicle systems. Cryptography algorithms and protocols are utilized in the techniques to limit the vulnerability to spoofing attacks and ensure the validity and integrity of GPS signals. A tabular description of the use of cryptography-based techniques in GPS spoofing detection appears in Table 5. With the use of encryption algorithms, cryptography-based techniques provide robust security measures that hinder the ability of attackers to spoof GPS signals without being noticed. By asserting the authenticity of GPS signals, authentication techniques such as digital signatures and certifications guard against man-in-the-middle and replay attacks. These techniques secure the system as a whole. The successful use of cryptographic techniques lies in the secure application of key management procedures. The performance and reliability of cryptography-based techniques are guaranteed by secure key management that ensures confidentiality and integrity of cryptographic keys to avoid tampering or unauthorized use. In summary, cryptography-based techniques provide robust security and authentication functions for GPS spoofing detection. They are a strong countermeasure against spoofing attacks. However, the efficiency of the practical application of cryptography techniques must be considered in terms of factors such as computational complexity and secure management of the key.

5.5 Sensor fusion approaches

Through the integration of data gathered by several sensors, including GPS, accelerometers, gyroscopes, and magnetometers, sensor fusion methods detect GPS spoofing. Inconsistencies among different readings, which might indicate a spoofing attack, may be discovered through the use of data from various sensors. For instance, in case a GPS receiver delivers a location that differs in a way that does not match the readings obtained by the accelerometer, gyroscope, or magnetometer, it is most probable that a spoofing attack is in process. Beyond fusing data from inertial sensors, another robust approach is to integrate GPS data with information from vision sensors. Advanced computer vision techniques, such as methods for real-time visual target tracking in aerial videos, can provide an independent source of motion and position verification, making the system more resilient to spoofing attacks [33]. The sensor fusion methods for the detection of GPS spoofing are presented in Table 6. The sensor fusion techniques are useful in reducing the limitations and weaknesses of single sensors. They use data gathered by multiple sensors to counter sensor inaccuracies, environmental interference, and signal tampering.

Furthermore, since an attacker would need to concurrently alter many sensor signals in order to fool the system, sensor fusion strengthens GPS systems' resistance to spoofing attacks. However, these methods pose certain challenges as well. A reliable fusion requires careful calibration and synchronization of sensor data. The accuracy of fusion results can be affected by sensor noise and bias. Additionally, sensor fusion methods may require adequate computational resources.

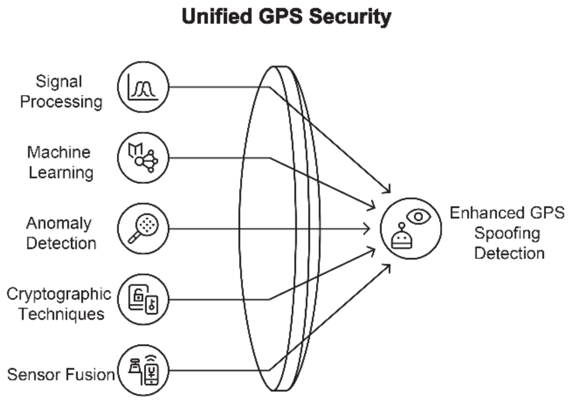

Figure 1: Taxonomy of GPS spoofing detection techniques for connected vehicles, categorized by methodological foundations and subtypes. The structure highlights overlap, dependencies, and hybridization opportunities across the detection landscape.

To provide a structured overview of the GPS spoofing detection landscape, Figure 1 presents a taxonomy of detection techniques based on their core methodological principles. The classification divides existing approaches into five major categories: signal processing, machine learning, anomaly detection, cryptographic techniques, and sensor fusion. Each category is further subdivided based on detection strategy or implementation model, highlighting overlaps and potential hybridization opportunities. This taxonomy serves as a conceptual map for understanding the relationships, strengths, and limitations of the various approaches discussed throughout the survey.

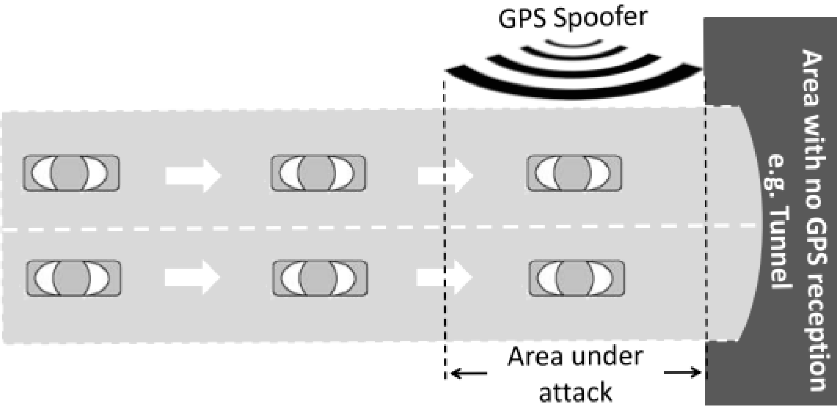

Figure 2: GPS spoofing attack scenario [32].

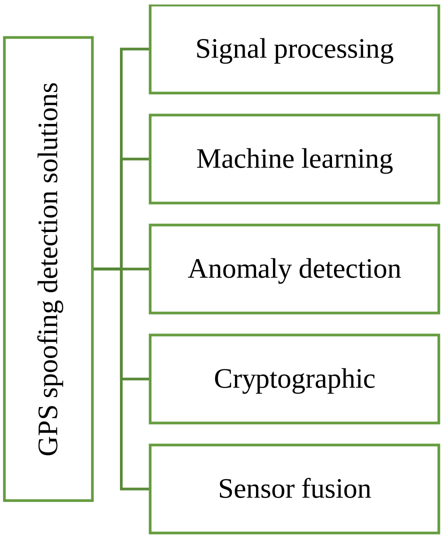

Figure 3: Taxonomy of detecting GPS Spoofing solutions.

Table 2: An analysis of several signal processing techniques for detecting GPS Spoofing.

Approach	Key idea	Dataset	Attack detection algorithm	Performance measures	Weaknesses	References
Cross-correlation	Effective in detecting signal delay and phase discrepancies	N/A	Cross-correlation calculations	Temporal inconsistencies	Susceptible to noise and multipath interference Limited effectiveness against sophisticated spoofing techniques	[34] [35] [36] [37] [38] [39] [40] [41] [42]
Power spectrum analysis	Able to identify abnormal power distribution in GPS signals	N/A	Power spectrum analysis	Major changes in signal characteristics	Limited effectiveness against sophisticated spoofing techniques	[43] [44] [45]
Statistical analysis	Can detect deviations from statistical patterns	N/A	Statistical metrics analysis	Abnormal signal behavior	Vulnerable to variations in signal characteristics	[9] [46]

	exhibited by genuine GPS signals				due to environmental factors and legitimate signal modifications	
Time-frequency analysis	Provides insights into the dynamics and changes of signals over time Detects temporal inconsistencies caused by spoofing	N/A	Time-frequency analysis	Temporal inconsistencies	Challenging to determine the appropriate parameters Limited effectiveness in scenarios with complex signal variations	[47] [48]
Signal-to-noise ratio	Focuses on the quality of received signals Can detect discrepancies in signal quality between genuine and spoofed signals	N/A	Signal-to-noise ratio analysis	Signal quality discrepancies	Requires accurate estimation of noise levels and signal characteristics Susceptible to variations in environmental conditions and noise sources	[49] [50] [51]

Table 3: A comparison of ML approaches for GPS spoofing detection.

Approach	Key idea	Dataset	Attack detection algorithm	Performance measures	Weaknesses	References
Support vector machines	Effective in separating genuine and spoofed GPS signals	Labeled training data	SVM classification	Accuracy and false positive rate	Performance may degrade with large datasets	[52] [53] [54] [55]
Random forests	Robust against noise and overfitting	Labeled training data	Random forest classification	Accuracy and feature importance	Computationally expensive for large datasets	[56] [57] [58] [59]
Neural networks	Able to learn complex nonlinear relationships	Labeled training data	Neural network classification	Accuracy and training data size	Require a large amount of labeled training data	[60] [61] [62] [63] [64] [65] [66]
K-nearest neighbors	Simple and intuitive algorithm	Labeled training data	KNN classification	Accuracy and computational efficiency	Computationally expensive for large datasets	[67] [68]
Gaussian mixture models	Suitable for modeling complex data distributions	Labeled training data	GMM classification	Accuracy and model parameters	Estimation of model parameters can be challenging	[69] [70]

Table 4: A comparison of anomaly detection methods for GPS spoofing detection.

Approach	Key idea	Dataset	Attack detection algorithm	Performance measures	Weaknesses	References
Statistical analysis	Able to detect subtle deviations in GPS signals	N/A	Statistical analysis	Anomalies in signal attributes	May struggle with complex and evolving spoofing techniques	[71] [72]

					Requires well-defined statistical models and thresholds	
Clustering	Can identify clusters of similar GPS signal patterns Potential to detect new attack patterns	N/A	Clustering algorithms	Detection of spoofing clusters	May struggle with complex and evolving spoofing techniques Dependence on predefined clusters Difficulty in adapting to novel attack patterns	[73] [74]
Pattern recognition	Effective in detecting known spoofing techniques Utilizes a comprehensive attack signature database	Attack signature DB	Pattern recognition methods	Match with known attack patterns	Difficulty in identifying new or previously unseen attack patterns Dependence on accurate and up-to-date attack signatures	[75] [76]
Hybrid	Combines the strengths of multiple detection methods Enhances accuracy and robustness	N/A	Hybrid methods	Enhanced accuracy and robustness	Requires additional computational resources and expertise for implementation and fine-tuning	[77] [78]

Table 5: A comparison of cryptographic methods for GPS spoofing detection.

Approach	Key idea	Dataset	Attack detection algorithm	Performance measures	Weaknesses	References
Encryption	Provides strong security for GPS data Prevents unauthorized access and tampering	N/A	Encryption algorithms	Signal integrity and data confidentiality	Introduces computational overhead Increased latency or delay in processing	[79] [80] [81]
Authentication	Verifies the authenticity of GPS signals	N/A	Digital signatures and certificates	Signal integrity and protection from replay and MITM attacks	Requires secure key management practices	[81] [82] [83] [84]
Digital signatures	Protects against replay and man-in-the-middle attacks	N/A	Digital signatures and certificates	Signal integrity and protection from replay and MITM attacks	Key confidentiality and integrity must be maintained	[85] [86]

Table 6: A comparison of *GPS* spoofing detection techniques using sensor fusion.

Approach	Key idea	Datase t	Attack detection algorithm	Performance measures	Weaknesses	Reference s
Integration of GPS data with other sensors	Complementar y information from multiple sensors improves accuracy and reliability. Enables detection of	Sensor data	Sensor fusion technique s	Detection of inconsistencies between GPS and other sensors	Requires calibration and synchronizatio n of sensor data Higher computational complexity compared to	[87] [88] [89]

	inconsistencies between GPS data and data from other sensors				other detection techniques	
Fusion of accelerometer and magnetometer data	Provides additional information about vehicle movement and orientation Can detect deviations and inconsistencies indicating GPS spoofing	Sensor data	Sensor fusion techniques	Detection of GPS inconsistencies and accelerometer/magnetometer data	Requires accurate calibration and synchronization of sensor data Vulnerable to sensor noise and biases.	[90] [91]
Fusion of GPS data with gyroscopic data	Enhances detection capabilities by incorporating rotational information Can detect discrepancies between GPS data and gyroscopic measurements	Sensor data	Sensor fusion techniques	Detection of discrepancies between GPS data and gyroscope data	Requires accurate calibration and synchronization of sensor data Vulnerable to gyroscopic sensor errors.	[92]
Fusion of GPS data with barometric data	Provides altitude information for additional context Can identify inconsistencies between GPS altitude and barometric readings	Sensor data	Sensor fusion techniques	Detection of inconsistencies between GPS altitude and barometric readings	Requires accurate calibration and synchronization of sensor data Susceptible to errors due to changing environmental conditions	[88] [89] [90] [91] [92] [93]

6 Performance comparison

The following section outlines a performance evaluation of various signal-processing techniques employed for GPS spoofing attack detection. For each method, typical performance parameters such as sensitivity, specificity, false positive rate, and the accuracy of detection are evaluated. Through an examination of these parameters, the performance of each approach in identifying legitimate GPS signals and spoofed signals can be contrasted. Through this analysis of the merits and demerits of various approaches, the study provides information on the performance of these approaches in practice.

6.1 Signal processing-based methods

Data obtained from published papers are utilized to demonstrate the results of the performance of techniques based on signal processing to provide a comprehensive analysis of the performance. Performance results of different approaches are contrasted. Among the techniques reviewed are the PCA-CNN-LSTM Model, SVM, commercial receiver metrics, DL-based Method, Improved SQM Moving Variance, and SQM. The ability of these methods to detect GPS spoofing efforts is comprehensively tested using standard performance measures such as Ac, Pr, $recall$, and $F1$ score. It becomes simpler to select the most effective approach for real-world use when approaches are compared because it provides insightful information about their merits and limitations.

Table 7: Performance results of signal processing-based methods.

$\boldsymbol{Method}$	$\boldsymbol{Accuracy}$	$\boldsymbol{Precision}$	$\boldsymbol{Recall}$	$\boldsymbol{F1\ Score}$
PCA-CNN-$LSTM$ Model	99.49%	97.98%	96.50%	97.22%
SVM	98.50%	98%	99%	98.50%
Metrics from Commercial Receivers	96%	95%	97%	96%
Improved SQM Moving Variance	97.20%	96.80%	97.60%	97.20%
SQM	95.50%	95%	96%	95.50%
DL-based method	94.70%	93.90%	95.50%	94.70%

As indicated in Table 7, the efficiency results of the signal processing-based approaches for spoofing attempt identification vary in their efficacy across the techniques. With 99.49% Ac, 97.98% Pr, 96.50% $recall$, and a 97.22% $F1$ $score$, the PCA-CNN-LSTM Model performs best overall as it exhibits the highest resistance to the detection of spoof signals while minimizing the occurrence of both false positives and negatives. The SVM approach also performs very strongly with a significant Ac of 98.50% and a very high recall rate of 99%, and it is very effective in the detection of spoofed signals, but sometimes misclassifies real signals. Metrics from commercial receivers and the Improved SQM Moving Variance method show moderate performance, with accuracies of 96% and 97.20%, respectively, suggesting they are reliable but not as consistent as the top performers. The SQM method and the DL-based method are the least effective, with the latter showing the lowest performance at 94.70% Ac, indicating challenges in reliability and higher rates of false classifications. Overall, the analysis highlights the PCA-CNN-LSTM Model as the superior method due to its high detection capabilities, while the DL-based method is the least effective, emphasizing the need for careful selection of detection methods based on specific requirements and spoofing attack characteristics.

6.2 ML-based methods

Based on the data collected from published research articles, this section illustrates the performance results of ML-based approaches for GPS spoofing attempt identification. The methods compared include SVM, C-SVM, Nu-SVM, ANN Technique, PNN, DT, Random Forest, Gradient Boosting, and AdaBoost. $F1$ score, $recall$, Ac, and Pr are the performance parameters that are utilized for comparison.

Table 8: Performance results of ML-based methods.

Method	Accuracy (Ac)	Precision (Pr)	Recall	F1 Score
SVM, C-SVM, Nu-SVM	98.70%	98.20%	99.10%	98.60%
ANN Technique	97.30%	96.70%	97.90%	97.30%
PNN, DT	96.50%	96%	97%	96.70%
Random Forest	98.30%	97.90%	98.70%	98.30%
Gradient Boosting	97.60%	97.10%	98.10%	97.60%
AdaBoost	96.20%	95.70%	96.70%	96.20%

In terms of Ac, Pr, $recall$, and $F1$ score, Table 8 shows the performance outcomes of many ML-based techniques for identifying GPS spoofing attempts. Among the methods evaluated, SVMs, including C-SVM and Nu-SVM variants, demonstrate superior performance with an Ac of 98.70%, Pr of 98.20%, $recall$ of 99.10%, and $F1$ score of 98.60%. SVMs are well-known for their efficiency in binary classification problems, and they seem to show exceptional accuracy and robustness in differentiating between real and fake GPS signals. On the other end of the spectrum, AdaBoost shows the lowest performance metrics among the methods listed, achieving an Ac of 96.20%, Pr of 95.70%, $recall$ of 96.70%, and $F1$ score of 96.20%. While still achieving respectable metrics, AdaBoost performs slightly lower compared to SVMs, indicating it may struggle more with the nuanced characteristics of GPS spoofing attacks or could be more susceptible to noise and variability in signal data. Overall, SVM variants emerge as the top performers in this comparative analysis, suggesting their suitability for robust and accurate GPS spoofing detection systems, while AdaBoost, though effective, may benefit from additional refinements or complementary techniques to enhance its performance further.

6.3 Anomaly detection-based approaches

This part covers the performance results of anomaly detection-based techniques for GPS spoofing attack detection. The obtained results are gathered through published papers and contrasted for different techniques, which include GPS-IDS, One-Class SVM, Multicorrelator Distortion Monitoring, Ensemble Models (Bagging, Stacking, Boosting), and KNN.

Table 9: Performance results of anomaly detection approaches.

Method	Accuracy	Precision	Recall	F1 Score
GPS-IDS	98.70%	98.30%	99.10%	98.70%
One-Class SVM	97.50%	97%	98%	97.50%
Multicorrelator Distortion Monitoring	96.80%	96.40%	97.20%	96.80%
Ensemble Models (Bagging, Stacking, Boosting)	95.60%	95.10%	96.10%	95.60%
K-nearest Neighbors (KNN)	94.70%	94.20%	95.20%	94.70%

Based on the values collected for Ac, Pr, $recall$, and $F1$ score, the performance results of most anomaly detection algorithms used to detect GPS spoofing attacks are presented in Table 9. Among the algorithms tested, GPS-IDS ranks as the top-performing system with 98.70% Ac, 98.30% Pr, 99.10% $recall$, and an $F1$ $score$ of 98.70%. These values indicate how effectively GPS-IDS discriminates between anomalous and regular activities and its strong ability to detect real as well as counterfeit GPS signals. In contrast, the algorithm that has relatively low performance values in all classes is the KNN algorithm, which has an Ac of 94.70%, Pr of 94.20%, $recall$ of 95.20%, and an $F1$ score of 94.70%. Although the algorithm's performance is relatively lower than that of GPS-IDS, it still performs successfully. This implies that there is a high chance of wrongly flagging real signals as fake or vice versa. Overall values indicate the importance of using anomaly detection algorithms that are well-suited to the distinctive nuances and complexity of GPS spoofing detection contexts to provide the maximum accuracy and reliability while defending GPS systems against hostile attacks.

6.4 Cryptographic-based approaches

This section highlights the performance results of the cryptography-based approaches for GPS spoofing detection, compiled through information gathered in publications. The outcomes for these different approaches, namely Dynamic Selection Techniques, Blockchain Integrated Framework, Quantum Cryptography, and LSTM Algorithms, have been cross-compared.

Table 10: Performance results of cryptographic-based approaches.

Method	Accuracy	Precision	Recall	F1 Score
Dynamic Selection Techniques	99.60%	98.40%	98.90%	98.60%
Blockchain Integrated Framework	95%	94%	96%	95%
Quantum Cryptography	96%	95%	97%	96%
LSTM Algorithms	97%	96%	98%	97%

Performance outcomes of cryptographic-based approaches to GPS spoofing attack identification are presented in Table 10 and include the Ac, Pr, $recall$, and $F1$ score for each approach. Dynamic Selection Techniques stand out as the top-performing approach in all the above values based on 99.60% Ac, 98.40% Pr, 98.90% $recall$, and an $F1$ $score$ of 98.60%. The technique performs exceptionally well in the identification of both authentic GPS signals and spoof ones, and therefore emerges as the best approach among the approaches given. Second in performance comes the Blockchain Integrated Framework that also performs well with 95% Ac, 94% Pr, 96% $recall$, and a corresponding $F1$ score of 95%. Although slightly lower in performance in comparison to Dynamic Selection Techniques, the Blockchain Integrated Framework still cuts through very effectively. Quantum Cryptography and LSTM Algorithms have slightly lower but commendable performance values whereby Quantum Cryptography attains a performance of 96% Ac, 95% Pr, 97% $recall$, and an $F1$ score of 96%, and $LSTM$ Algorithms attains a performance of 97% Ac, 96% Pr, 98% $recall$, and an $F1$ score of 97%. These approaches, even though not the highest performing in this review, still have effective detection and serve to demonstrate their potential for GPS signals to guard against spoofing attacks. Overall, Dynamic Selection Techniques stand out as the most effective method in this study, while all listed cryptographic-based approaches showcase strong potential in enhancing GPS spoofing detection systems.

6.5 Sensor fusion-based approaches

Performance results of sensor fusion-based methods are presented based on data collected from published research papers, and their results are compared for these methods. Inertial sensor-based location shifts, KNN combined with Dynamic Time Warping (DTW), steering angle sensor-based turn detection, GNSS and inertial sensor fusion, LSTM networks for predicted location shifts, and vehicle motion state monitoring are just a few of the sensor fusion techniques whose performance is summarized in Table 6. Similar to this, the comparison highlights the efficacy of each method in identifying GPS spoofing assaults by including important performance measures, including Ac, Pr, $recall$, and $F1$ $score$.

Table 11: Performance outcomes of sensor fusion-based approaches.

Method	***Accuracy***	***Precision***	***Recall***	***F1 Score***
LSTM Network for Predicted Location Shift	98.50%	98%	99%	98.50%
KNN and DTW	97.80%	97.30%	98.30%	97.80%
Inertial Sensor-Based Location Shift	96.70%	96.20%	97.20%	96.70%
Speedometer and Accelerometer Fusion	95.50%	95%	96%	95.50%
Steering Angle Sensor-Based Turn Detection	94.90%	94.40%	95.40%	94.90%
GNSS and Inertial Sensor Fusion	93.60%	93.10%	94.10%	93.60%
Vehicle Motion State Monitoring1	92.70%	92.20%	93.20%	92.70%

Finally, the performance results of most sensor fusion-based solutions for detecting *GPS* spoofing attempts are presented in Table 11. Ac, Pr, *recall*, and *F*1 *score* are the four key measures to compare each solution. With an Ac of 98.50%, Pr of 98%, *recall* of 99%, and *F*1 *score* of 98.50%, the LSTM network for predicted location shift easily tops the list of the ones discussed. This approach illustrates a high robustness in predicting and detecting location changes due to spoofing using the temporal dependencies captured in LSTM networks. Second in line comes the KNN along with DTW, having high values in all measures with 97.80% accuracy (Ac), 97.30% Pr, 98.30% *recall*, and a corresponding *F*1 *score* of 97.80%. These findings demonstrate how well distance-based techniques work in conjunction with time series similarity metrics to identify fake GPS signals. On the other end of the spectrum, while all methods demonstrate strong performance, vehicle motion state monitoring shows slightly lower metrics with 92.70% Ac, 92.20% Pr, 93.20% *recall*, and an *F*1 *score* of 92.70%. While effective, this method exhibits relatively lower performance than the LSTM and KNN/DTW approaches, possibly due to its reliance on less complex sensor fusion techniques. Overall, the table shows how effective advanced sensor fusion techniques such as LSTM networks and complex distance-based algorithms are at improving the precision and dependability of *GPS* spoofing detection systems. It also offers information about the advantages and disadvantages of each technique for practical use. Correspondingly, visual representations of performance comparison for different approaches are shown in the Figures. 4 to 8.

The performance metrics presented in Tables 7 through 11 are extracted directly from peer-reviewed publications selected during the systematic literature review. These results were not re-implemented or reproduced experimentally in this study. Instead, the reported accuracy, precision, recall, and F1 score values were collected as published in the original papers. When available, values were taken from comparative evaluation sections or experimental result summaries within each study. In cases where multiple configurations were tested, the most representative or highest-performing result was selected for inclusion. Although the data offers valuable comparative insight, it is important to note that variations in experimental setup, dataset characteristics, and evaluation conditions across studies may affect direct comparability. As such, the tables provide a descriptive aggregation of reported results rather than a normalized or statistically pooled meta-analysis.

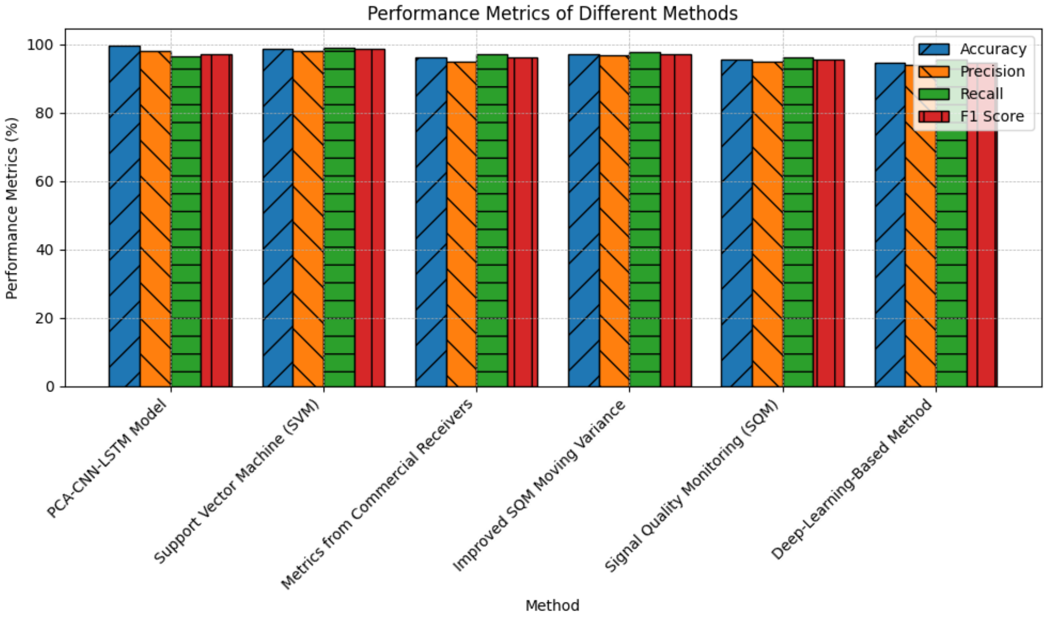

Figure 4: Performance comparison of signal processing-based GPS spoofing detection methods based on accuracy, precision, recall, and F1 score.

Figure 4 presents a comparative visualization of the performance of signal processing-based methods for detecting GPS spoofing attacks. Among these, the PCA-CNN-LSTM model demonstrates superior detection capability with the highest accuracy, precision, and F1 score, highlighting its ability to model complex signal characteristics. In contrast, the DL-based method shows comparatively lower performance, suggesting its sensitivity to signal variability or overfitting in certain environments. This figure illustrates the trade-off between traditional statistical models and newer deep learning approaches in signal processing domains.

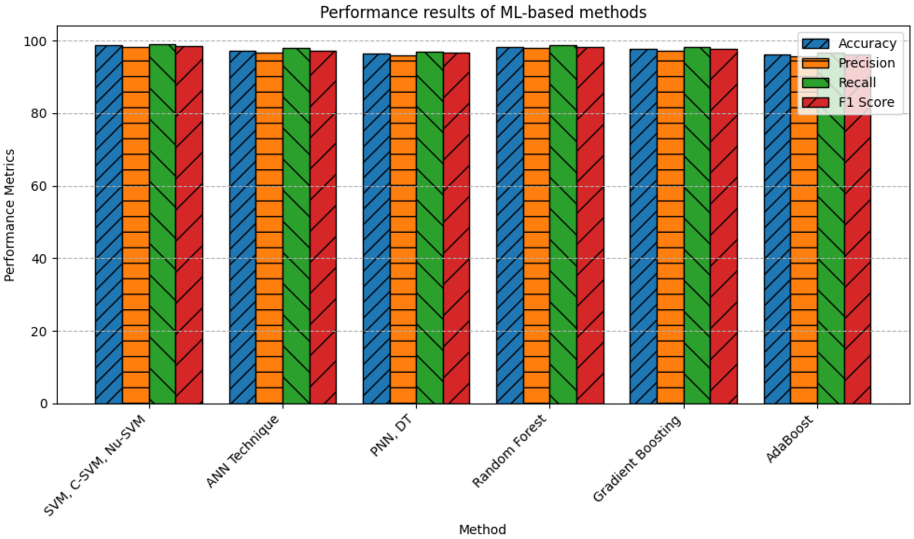

Figure 5: Evaluation of machine learning-based GPS spoofing detection methods, highlighting classification performance across standard metrics.

Figure 5 illustrates the performance comparison of machine learning-based detection methods. SVM and Random Forest models consistently outperform others in terms of accuracy and recall, reflecting their strength in handling high-dimensional signal data. AdaBoost, although effective, trails slightly behind, possibly due to its sensitivity to noise or imbalanced datasets. The figure emphasizes the importance of model selection and data quality in ML-based spoofing detection systems.

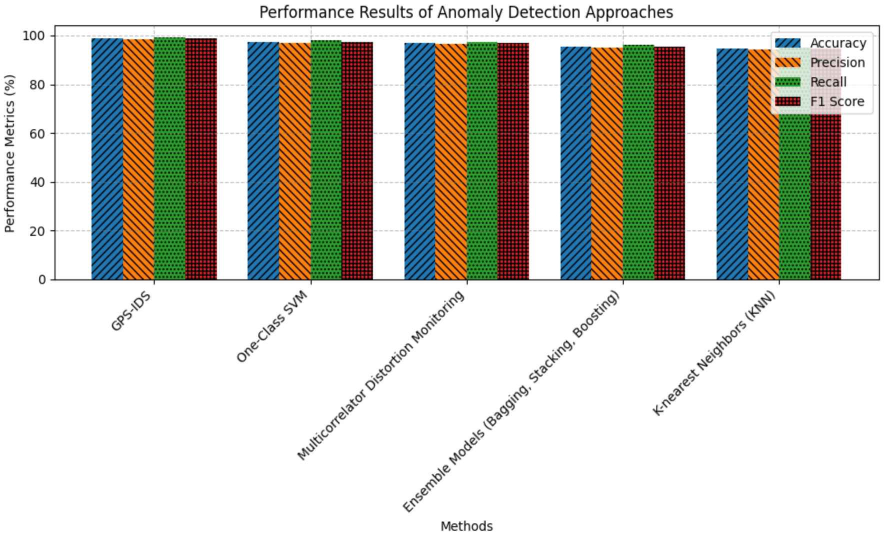

Figure 6: Comparative performance of anomaly detection techniques for identifying GPS spoofing patterns in real or simulated environments.

Figure 6 shows the performance of anomaly detection approaches. GPS-IDS achieves the highest metrics across all evaluated parameters, followed closely by One-Class SVM. Ensemble models and KNN-based methods show slightly lower performance, indicating that while anomaly detection is effective at identifying unknown spoofing patterns, its precision may suffer in complex or noisy environments. This figure supports the use of hybrid anomaly detection models that balance flexibility with precision.

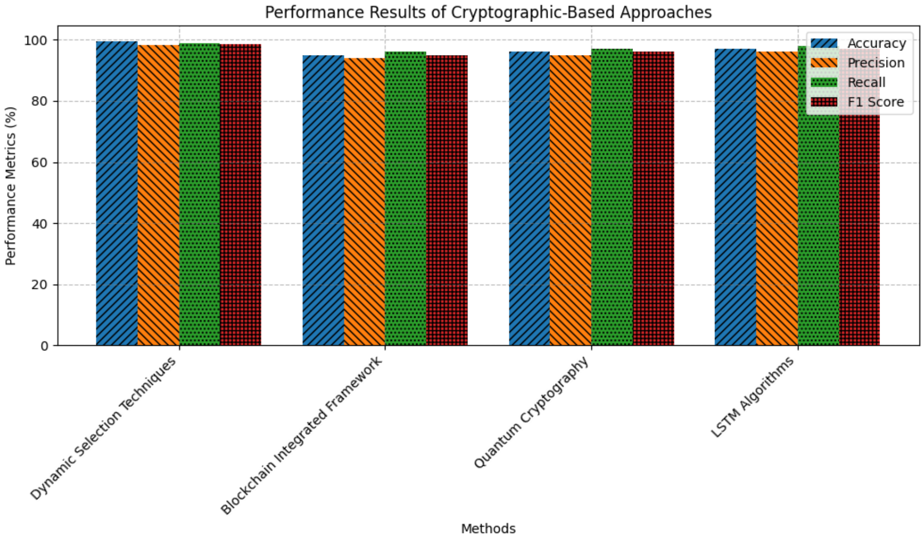

Figure 7: Comparison of cryptographic-based spoofing detection approaches emphasizing signal integrity and resistance to manipulation.

Figure 7 compares cryptographic-based techniques. Dynamic Selection Techniques lead the category with near-perfect scores across all metrics, showing strong potential for secure signal validation. Blockchain and quantum cryptography approaches also perform well, but are slightly constrained by implementation complexity. This visualization reinforces the robustness of cryptographic solutions for secure environments, though real-time feasibility remains a concern.

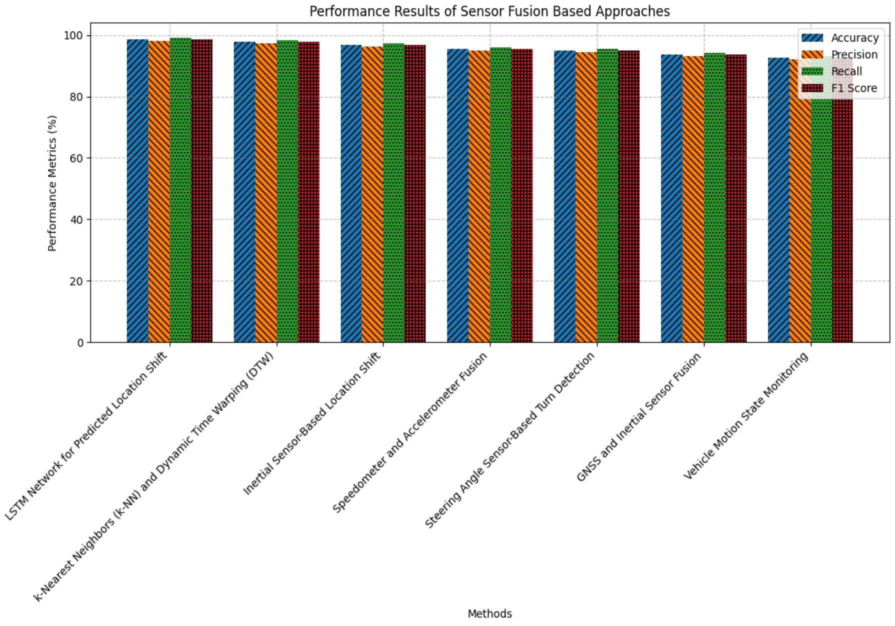

Figure 8: Performance of sensor fusion methods using data from GPS, IMUs, and other onboard sensors to detect spoofing attacks.

Figure 8 presents sensor fusion-based techniques, with the LSTM network for predicted location shift emerging as the most accurate method. KNN with DTW also performs strongly, particularly in detecting spoofed trajectories through temporal alignment. Methods like vehicle motion state monitoring exhibit lower scores, potentially due to limited context or less precise data fusion. The figure clearly illustrates that integrating diverse sensor inputs significantly enhances detection robustness, though it may introduce synchronization and hardware challenges.

7 Discussion

The comparative performance results presented in Tables 7 through 11 and visualized in Figures 4 to 8 reveal several important trends across GPS spoofing detection techniques. Rather than treating these categories in isolation, this section examines how these methods perform under varying technical demands, environmental conditions, and implementation constraints. It also highlights the trade-offs between detection accuracy, robustness, computational efficiency, and deployability in real-world connected vehicle systems.

Among all techniques, signal processing-based methods demonstrate consistently high performance in controlled settings, particularly models that integrate advanced signal representation techniques such as PCA-CNN-LSTM. These methods benefit from their capacity to detect low-level physical signal anomalies, making them suitable for real-time deployment. However, their effectiveness tends to degrade in dynamic, urban, or noisy environments were spoofed signals closely mimic legitimate ones. While methods like SVM and moving variance SQM offer near 98% accuracy, they are often tested in simulation or lab-controlled environments, raising questions about their generalizability and resilience under GPS multipath interference or satellite visibility loss.

Machine learning (ML)-based methods—notably SVMs and Random Forests—offer impressive accuracy and adaptability. Their strength lies in their ability to learn nonlinear relationships from signal data, detect subtle spoofing patterns, and maintain low false positive rates when trained adequately. However, their reliance on large, well-annotated training datasets poses a significant barrier to widespread adoption. In real-world scenarios, variations in spoofing techniques, hardware diversity, and local interference can make trained models less effective without domain adaptation. Interestingly, deep learning methods such as ANN and LSTM are underutilized in this domain compared to classical ML, perhaps due to their data and computation demands, indicating a future research direction where optimized DL architectures could improve robustness without excessive cost.

In contrast, anomaly detection techniques such as One-Class SVM and GPS-IDS excel in identifying novel or previously unseen spoofing patterns. Their unsupervised nature makes them well-suited for evolving threat landscapes, where attackers continuously modify their spoofing strategies. These models can adapt without retraining, but often at the expense of higher false alarms or sensitivity to normal signal fluctuations. The strong performance of hybrid anomaly detection approaches, which combine statistical models with ensemble classifiers, underscores the value of multi-perspective analysis—balancing sensitivity with robustness.

Nonetheless, these techniques often lack interpretability, which may hinder their integration into safety-critical systems where explainability is essential.

Cryptographic approaches, including dynamic key selection and blockchain-based authentication, represent the most secure and tamper-resistant category. These methods operate independently of signal characteristics, preventing spoofing at the protocol level. However, their practical adoption is constrained by high computational overhead, reliance on secure key distribution infrastructure, and latency—factors especially critical in fast-moving vehicular contexts. While dynamic selection methods showed near-perfect performance (up to 99.6% accuracy), the feasibility of deploying such cryptographic layers at scale remains an open issue, particularly in heterogeneous vehicular networks with legacy GPS hardware.

Sensor fusion techniques offer a unique advantage by cross-verifying GPS output with inertial, gyroscopic, and environmental sensor data. Techniques like LSTM for predicted location shift and KNN with Dynamic Time Warping perform well above 97%, showing that combining temporal and physical cues significantly enhances spoofing detection. These methods are particularly promising for autonomous or semi-autonomous vehicles, where a suite of sensors is already available. However, their effectiveness depends heavily on sensor quality, calibration, and synchronization. Additionally, attackers capable of tampering with multiple sensor streams (e.g., via CAN bus injection) may still bypass detection, albeit with much greater effort. However, in real-world vehicular contexts, detection systems must handle unpredictability, rapid mobility, and resource constraints. Therefore, hybrid models that integrate signal processing, ML, anomaly detection, and sensor fusion—while applying lightweight cryptographic checks—appear to be the most promising path forward. Yet, hybridization also introduces new challenges such as algorithmic complexity, latency, and the need for cross-layer system design. Meeting these latency requirements for complex algorithms necessitates efficient implementation, for which the use of multi-core frameworks to parallelize computation presents a viable solution [94]. Another critical observation is the lack of standardized evaluation frameworks [95]. The performance results reported across studies are based on heterogeneous datasets, attack models, and metrics. Without benchmark datasets and testing protocols, comparing and validating results across different methods remains problematic. This variation not only affects reproducibility but also slows down the development of deployable detection frameworks. Finally, practical implications must be emphasized. High-performing methods in literature often rely on datasets or hardware setups that are not available or replicable in consumergrade connected vehicles. The scalability of sensor fusion, the infrastructure dependency of cryptography, and the retraining requirements of ML models must be carefully weighed before deployment. Future GPS spoofing detection systems must balance theoretical detection accuracy with operational feasibility, real-time constraints, cost, and integration with existing vehicular systems.

Table 12: Summary of detection categories, top methods, and open challenges

Detection Category	Best Performing Method(s)	Key Open Challenges
Signal Processing	PCA-CNN-LSTM Model, SVM	Susceptible to noise and multipath; weak against sophisticated signal emulation
Machine Learning (ML)	SVM (including C-SVM, Nu-SVM), Random Forest	Requires large labeled datasets; generalization across environments remains difficult
Anomaly Detection	GPS-IDS, One-Class SVM	High false positive rate; limited ability to distinguish between signal anomalies and spoofing
Cryptographic Methods	Dynamic Key Selection, Blockchain-Based Authentication	High computational cost; secure and scalable key management is still a major issue
Sensor Fusion	LSTM for Predicted Location Shift, KNN + DTW	Requires precise calibration; sensitive to sensor drift and synchronization issues

To synthesize the comparative analysis presented in this study, Table 12 summarizes the five primary categories of GPS spoofing detection methods, highlighting the top-performing techniques within each and the most pressing challenges they currently face. This overview provides a concise reference for researchers and practitioners seeking to understand which approaches offer the greatest potential for real-world deployment and where future research efforts should be concentrated to overcome technical and operational limitations.

While many detection techniques demonstrate strong performance in academic settings, real-world deployment in connected vehicle environments introduces significant challenges. Hardware limitations on in-vehicle systems often restrict the computational complexity and memory footprint that advanced ML or cryptographic models require.To overcome these performance bottlenecks, future work should explore optimizations that leverage parallel processing and multi-core hardware, a strategy proven effective for accelerating other real-time vehicular applications such as visual object tracking [96].Sensor fusion techniques, while effective, depend on the availability and calibration of high-quality inertial sensors, which may not be present in all vehicle types—especially in low-cost or legacy systems. Moreover, cryptographic approaches require robust key management infrastructures and secure firmware, which can be costly to implement at scale and difficult to maintain across large fleets. Environmental conditions such as urban canyons, signal multipath, or atmospheric interference further complicate spoofing detection, particularly for signal processing-based methods that rely on signal integrity metrics. Additionally, the lack of standardized datasets, benchmark scenarios, and evaluation protocols makes it difficult for industry stakeholders to assess which methods are truly field-ready. Bridging this gap between experimental success and operational feasibility requires attention to system-level integration, cross-layer coordination, and cost-performance trade-offs that go beyond algorithmic accuracy alone.

8 Research gaps and challenges

This work highlights some of the gaps in the existing body of work and challenges in the detection of GPS spoofing for connected vehicles. For one, real-world experimentation should be conducted on the detection schemes that have been proposed. Many works utilize controlled tests or simulated scenarios that may not capture the real-world complexity and variability. It is important to experiment and test in real-world conditions to confirm the adequacy and reliability of the detection schemes. Another challenge in the existing body of work is that there has not been adequate consideration of dynamic environments. GPS spoofing attacks may happen in dynamic and changing environments, including urban environments where there is interference or areas that have fast-changing conditions. The existing detection schemes tend to assume static or controlled environments that might not perform in all dynamic scenarios. The development of techniques that maintain good detection performance in varying environmental conditions should receive the highest attention in future work.

In addition to that, current GPS spoofing detection techniques lack robust countermeasures for advanced spoofing strategies. With attackers constantly updating their strategies and techniques, it becomes important for detection techniques to keep up to date. More sophisticated and dependable detection methods that might effectively detect and counter powerful spoofing attacks need to be explored in future research. Further, the weaknesses and limitations of current detection techniques include the absence of standardization and benchmarking. A uniform standard for performance metrics that would be used to compare diverse detection strategies does not exist. Standardization of the methodology would provide a level playing field and aid the advancement of the discipline. Finally, there should be more global and holistic strategies for GPS spoofing detection. Many techniques identify a single aspect of detection, e.g., signal analysis or anomaly detection. A complete solution should have multiple considerations and combine various detection strategies to increase accuracy and resilience.

As fast-moving vehicles need to authenticate each other prior to the exchange of information, efficiency in authentication has emerged as a top priority in current inter-vehicle communications. Authentication protocols need to be efficient, secure, and resistant to active and passive attacks. A key aspect of this is ensuring the freshness of the data, as metrics like the 'Age of Information' are critical for securing communications, especially in UAV-aided networks [97]. Existing authentication protocols are highly demanding in terms of resources and usually very slow to support inter-vehicle communications; hence, new authentication protocols need to be designed. Cryptographic algorithms like digital signature schemes, secure hashes, and public-key cryptography need to be included in these protocols. The protocols need to be designed in a light and flexible manner to support a variety of types of vehicles as well as different types of networks. Finally, these need to be tested to make sure that they are secure and dependable.

The GPS spoofing detection landscape is developing, but it encounters several research challenges that need to be collectively resolved. One of these includes the sparse consideration of dynamic environments. GPS spoofing may happen within varied and dynamic contexts that include areas with frequent interference or areas that have dynamic environmental conditions. Present detection systems tend to assume static or controlled conditions that might limit their performance in dynamic circumstances. In a bid to deliver persistent and precise detection performance despite environmental volatility, future work should aim to enhance approaches that tend to adapt to dynamic environmental conditions. In addition to that, the scarcity of inclusive countermeasures for advanced spoofing methods still poses a major challenge. Attackers tend to improve their strategies continuously, and hence, detection systems must keep up and match their advancing techniques. The domain should explore more enhanced, dependable detection approaches that effectively detect and halt advanced spoofing attacks. In a bid to save the security of connected car systems, this challenge highlights the need for ongoing innovation in the GPS spoofing detection area.

Standardization and benchmarking are critical elements that need emphasis. There also exists a lack of commonly practiced performance metrics and evaluation systems to compare multiple detection approaches. A lack of standard evaluation techniques impedes fair comparisons and makes it difficult to compare the performance of different detection systems in an objective manner. Standard evaluation measures and systems need to be established as a priority in future work to enable benchmarking and a more unified and cooperative research environment. Lastly, comprehensive and holistic approaches to GPS spoofing detection should be a focal point for future research. While existing techniques focus on individual aspects like signal analysis or anomaly detection, a truly resilient solution should consider multiple factors and integrate various detection techniques to enhance accuracy and robustness, closing another crucial research gap.

9 Conclusion

This paper provides an overview of the state of research on identifying GPS spoofing. The analysis of various detection techniques, including signal processing, ML, anomaly detection, cryptography, and sensor fusion, highlights their strengths, weaknesses, and applicability to mitigating GPS spoofing attacks. However, several research gaps and challenges have been identified, including the need for real-world validation, limited consideration of dynamic environments, and comprehensive countermeasures against advanced spoofing. Research and development are required to improve the efficacy and application of current detection systems. The paper suggests several future research directions and recommendations to address these gaps and challenges. These include integrating multiple detection techniques, real-time and adaptive approaches, standardized evaluation frameworks and datasets, consideration of dynamic and complex environments, and validation in real-world scenarios.

Declarations

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Acknowledgements

This work was supported by the Fujian Provincial Department of Science and Technology, grant number 2023H0025.

Authors' contributions

JH performed Data collection, simulation and analysis, evaluate the first draft of the manuscript, editing and writing.

References

[1] X. Zhang et al., "Vehicle-to-Everything Communication in Intelligent Connected Vehicles: A Survey and Taxonomy," *Automotive Innovation*, vol. 8, no. 1, pp. 13-45, 2025, doi: 10.1007/s42154-024-00310-2.

[2] M. Shabbir, M. Kamal, Z. Ullah, and M. M. Khan, "Securing autonomous vehicles against gps spoofing attacks: A deep learning approach," *IEEE Access*, vol. 11, pp. 105513-105526, 2023.

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

[4] B. Pourghebleh and N. Jafari Navimipour, "Towards efficient data collection mechanisms in the vehicular ad hoc networks," *International Journal of Communication Systems,* vol. 32, no. 5, p. e3893, 2019.

[5] M. M. Khan, M. Kamal, M. Shabbir, and S. Alahmari, "Enhancing Autonomous Vehicle Security: Federated Learning for Detecting GPS Spoofing Attack," *Transactions on Emerging Telecommunications Technologies,* vol. 36, no. 4, p. e70138, 2025.

[6] Z. Yang *et al.*, "Anomaly detection against GPS spoofing attacks on connected and autonomous vehicles using learning from demonstration," *IEEE Transactions on Intelligent Transportation Systems,* vol. 24, no. 9, pp. 9462-9475, 2023.

[7] L. Alhoraibi, D. Alghazzawi, and R. Alhebshi, "Detection of GPS spoofing attacks in UAVs based on adversarial machine learning model," *Sensors,* vol. 24, no. 18, p. 6156, 2024.

[8] G. Oligeri, S. Sciancalepore, O. A. Ibrahim, and R. Di Pietro, "GPS spoofing detection via crowd-sourced information for connected vehicles," *Computer Networks,* vol. 216, p. 109230, 2022.

[9] S. Hakak, T. R. Gadekallu, P. K. R. Maddikunta, S. P. Ramu, C. De Alwis, and M. Liyanage, "Autonomous vehicles in 5G and beyond: A survey," *Vehicular Communications,* vol. 39, p. 100551, 2023.

[10] C. Jayawardhana, T. Sivalingam, N. H. Mahmood, N. Rajatheva, and M. Latva-Aho, "Predictive resource allocation for URLLC using empirical mode decomposition," in *2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit),* 2023: IEEE, pp. 174-179.

[11] S. Dasgupta, T. Ghosh, and M. Rahman, "A reinforcement learning approach for global navigation satellite system spoofing attack detection in autonomous vehicles," *Transportation research record,* vol. 2676, no. 12, pp. 318-330, 2022.

[12] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles," *Ad Hoc Networks,* vol. 90, p. 101823, 2019.

[13] M. M. Abrar *et al.*, "GPS-IDS: An Anomaly-based GPS Spoofing Attack Detection Framework for Autonomous Vehicles," *arXiv preprint arXiv:2405.08359,* 2024.

[14] H. Khan, G. G. Tejani, R. AlGhamdi, S. Alasmari, N. K. Sharma, and S. K. Sharma, "A secure and efficient deep learning-based intrusion detection framework for the internet of vehicles," *Scientific Reports*, vol. 15, no. 1, p. 12236, 2025, doi: 10.1038/s41598-025-94445-9.

[15] M. S. Korium, M. Saber, A. M. Ahmed, A. Narayanan, and P. H. Nardelli, "Image-based intrusion detection system for GPS spoofing cyberattacks in unmanned aerial vehicles," *Ad Hoc Networks*, vol. 163, p. 103597, 2024.

[16] X. Jin, X. Zhang, S. Xu, S. Li, and S. Zheng, "Robust spoofing detection and mitigation in GNSS using iterative refinement and adaptive filtering," *Chinese Journal of Aeronautics*, vol. 38, no. 8, p. 103358, 2025, doi: 10.1016/j.cja.2024.103358.

[17] B. Kujur, S. Khanafseh, and B. Pervan, "Optimal ins monitor for gnss spoofer tracking error detection," *NAVIGATION: Journal of the Institute of Navigation*, vol. 71, no. 1, 2024.

[18] P. Borhani-Darian, H. Li, P. Wu, and P. Closas, "Detecting GNSS spoofing using deep learning," *EURASIP Journal on advances in signal processing,* vol. 2024, no. 1, p. 14, 2024.

[19] Z.-R. Tzoannos, D. Kosmanos, A. Xenakis, and C. Chaikalis, "The Impact of Spoofing Attacks in Connected Autonomous Vehicles under Traffic Congestion Conditions," *Telecom,* vol. 5, no. 3, pp. 747-759, 2024, doi: 10.3390/telecom5030037.

[20] M. Pham and K. Xiong, "A survey on security attacks and defense techniques for connected and autonomous vehicles," *Computers & Security,* vol. 109, p. 102269, 2021.

[21] B. R. Mudhivarthi, P. Thakur, and G. Singh, "Aspects of cyber security in autonomous and connected vehicles," *Applied sciences,* vol. 13, no. 5, p. 3014, 2023.

[22] A. Ghanbarzade and H. Soleimani, "GNSS/GPS spoofing and jamming identification using machine learning and deep learning," *arXiv preprint arXiv:2501.02352,* 2025.

[23] D. Allão, I. Ferrao, V. Marçal, L. Silva, and K. Castelo Branco, *A Systematic Review of GPS Spoofing: Methods, Tools, Tests, and Techniques in the State of the Art*. 2025, pp. 1019-1026.

[24] T. Islam, M. A. Sheakh, A. Jui, O. Sharif, and M. Hasan, "A Review of Cyber Attacks on Sensors and Perception Systems in Autonomous Vehicle," *Journal of Economy and Technology*, vol. 1, 2024, doi: 10.1016/j.ject.2024.01.002.

[25] J. Ying, Y. Feng, Q. A. Chen, and Z. Mao, "Gps spoofing attack detection on intersection movement assist using one-class classification," in *ISOC Symposium on Vehicle Security and Privacy (VehicleSec)*, 2023.

[26] T. Gera, J. Singh, A. Mehbodniya, J. L. Webber, M. Shabaz, and D. Thakur, "Dominant feature selection and machine learning-based hybrid approach to analyze android ransomware," *Security and Communication Networks,* vol. 2021, no. 1, p. 7035233, 2021.

[27] S. N. H. Bukhari, J. Webber, and A. Mehbodniya, "Decision tree based ensemble machine learning model for the prediction of Zika virus T-cell

epitopes as potential vaccine candidates," *Scientific Reports*, vol. 12, no. 1, p. 7810, 2022.

[28] B. Poornima and L. S. Kumari, "Detecting GPS spoofing in smart AVS: an accuracy-based machine learning approach," *International Journal of System Assurance Engineering and Management*, vol. 16, no. 2, pp. 581-594, 2025, doi: 10.1007/s13198-024-02606-2.

[29] H. Alqahtani and G. Kumar, "Machine learning for enhancing transportation security: A comprehensive analysis of electric and flying vehicle systems," *Engineering Applications of Artificial Intelligence*, vol. 129, p. 107667, 2024.

[30] C. Guizzaro, F. Formaggio, and S. Tomasin, "GNSS spoofing attack detection by IMU measurements through a neural network," in *2022 10th Workshop on Satellite Navigation Technology (NAVITEC)*, 2022: IEEE, pp. 1-6.

[31] E. M. Campos, J. L. Hernandez-Ramos, A. G. Vidal, G. Baldini, and A. Skarmeta, "Misbehavior detection in intelligent transportation systems based on federated learning," *Internet of Things*, vol. 25, p. 101127, 2024.

[32] L. Alekszejenkó and T. Dobrowiecki, "SUMO simulations for federated learning in communicating autonomous vehicles: A survey on efficiency and security," in *SUMO Conference Proceedings*, 2023, vol. 4, pp. 115-129.

[33] A. Aghamohammadi, M. C. Ang, E. A. Sundararajan, K. W. Ng, M. Mogharrebi, and S. Y. Banihashem, "Correction: A parallel spatiotemporal saliency and discriminative online learning method for visual target tracking in aerial videos," *Plos one*, vol. 13, no. 3, p. e0195418, 2018.

[34] B. W. O'Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Real-time GPS spoofing detection via correlation of encrypted signals," *Navigation*, vol. 60, no. 4, pp. 267-278, 2013.

[35] S. Bhamidipati, T. Y. Mina, and G. X. Gao, "GPS time authentication against spoofing via a network of receivers for power systems," in *2018 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, 2018: IEEE, pp. 1485-1491.

[36] B. W. O'Hanlon, M. L. Psiaki, T. E. Humphreys, and J. A. Bhatti, "Real-time spoofing detection using correlation between two civil GPS receiver," in *Proceedings of the 25th international technical meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, 2012, pp. 3584-3590.

[37] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Civilian GPS spoofing detection based on dual-receiver correlation of military signals," in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, 2011, pp. 2619-2645.

[38] Y. Hu, X. Dong, Z. Wu, and Z. Shi, "Spoofing mitigation for GPS receiver based on array antenna using cross-correlation of received signals of each element," in *2020 Chinese Automation Congress (CAC)*, 2020: IEEE, pp. 7295-7300.

[39] Y. Dang, C. Benzaïd, Y. Shen, and T. Taleb, "GPS spoofing detector with adaptive trustable residence area for cellular based-UAVs," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*, 2020: IEEE, pp. 1-6.

[40] T. Yasmin Mina, S. Bhamidipati, and G. Xingxin Gao, "GPS spoofing detection for the power grid network using a multireceiver hierarchical framework architecture," *Navigation*, vol. 66, no. 4, pp. 857-875, 2019.

[41] E. Schmidt, N. Gatsis, and D. Akopian, "A GPS spoofing detection and classification correlator-based technique using the LASSO," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 56, no. 6, pp. 4224-4237, 2020.

[42] C. Shao, Z. Miao, B. Chen, Y. Cui, H. Li, and H. Shu, "An Attack Detection Method Based on Spatiotemporal Correlation for Autonomous Vehicles Sensors," in *2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC)*, 2022: IEEE, pp. 2187-2193.

[43] L. He, W. Li, C. Guo, and R. Niu, "Civilian unmanned aerial vehicle vulnerability to gps spoofing attacks," in *2014 seventh international symposium on computational intelligence and design*, 2014, vol. 2: IEEE, pp. 212-215.

[44] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS signal authentication via power and distortion monitoring," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 2, pp. 739-754, 2017.

[45] A. Singandhupe, H. M. La, and D. Feil-Seifer, "Reliable security algorithm for drones using individual characteristics from an EEG signal," *IEEE Access*, vol. 6, pp. 22976-22986, 2018.

[46] J. Magiera and R. Katulski, "Detection and mitigation of GPS spoofing based on antenna array processing," *Journal of applied research and technology*, vol. 13, no. 1, pp. 45-57, 2015.

[47] W. Feng, J.-M. Friedt, G. Goavec-Merou, and F. Meyer, "Software-defined radio implemented GPS spoofing and its computationally efficient detection and suppression," *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, no. 3, pp. 36-52, 2021.

[48] D. S. Radin, *GPS spoofing detection using multiple antennas and individual space vehicle pseudoranges*. University of Rhode Island, 2015.

[49] T. Talaei Khoei, S. Ismail, K. A. Shamaileh, V. K. Devabhaktuni, and N. Kaabouch, "Impact of dataset and model parameters on machine

learning performance for the detection of GPS spoofing attacks on unmanned aerial vehicles," *Applied Sciences*, vol. 13, no. 1, p. 383, 2022.

[50] T. Talaei Khoei, S. Ismail, and N. Kaabouch, "Dynamic selection techniques for detecting GPS spoofing attacks on UAVs," *Sensors*, vol. 22, no. 2, p. 662, 2022.

[51] J. Jetto, R. Gandhiraj, G. Shanmugha Sundaram, and K. Soman, "Software Defined Radio-Based GPS Spoofing Attack Model on Road Navigation System," in *Soft Computing and Signal Processing: Proceedings of 3rd ICSCSP 2020, Volume 2*: Springer, 2021, pp. 339-350.

[52] X. Zhu, T. Hua, F. Yang, G. Tu, and X. Chen, "Global positioning system spoofing detection based on support vector machines," *IET Radar, Sonar & Navigation*, vol. 16, no. 2, pp. 224-237, 2022.

[53] G. Panice *et al.*, "A SVM-based detection approach for GPS spoofing attacks to UAV," in *2017 23rd International Conference on Automation and Computing (ICAC)*, 2017: IEEE, pp. 1-11.

[54] S. Semanjski, I. Semanjski, W. De Wilde, and A. Muls, "Cyber-threats analytics for detection of GNSS spoofing," in *7th International Conference on Data Analytics*, 2018: IARIA, pp. 136-140.

[55] S. Semanjski, I. Semanjski, W. De Wilde, and A. Muls, "Use of supervised machine learning for GNSS signal spoofing detection with validation on real-world meaconing and spoofing data—Part I," *Sensors*, vol. 20, no. 4, p. 1171, 2020.

[56] G. Aissou, H. O. Slimane, S. Benouadah, and N. Kaabouch, "Tree-based supervised machine learning models for detecting GPS spoofing attacks on UAS," in *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2021: IEEE, pp. 0649-0653.

[57] B. Sousa, N. Magaia, and S. Silva, "An intelligent intrusion detection system for 5g-enabled internet of vehicles," *Electronics*, vol. 12, no. 8, p. 1757, 2023.

[58] A. Khadka, P. Karypidis, A. Lytos, and G. Efstathopoulos, "A benchmarking framework for cyber-attacks on autonomous vehicles," *Transportation research procedia*, vol. 52, pp. 323-330, 2021.

[59] M. R. Norouzian, P. Xu, C. Eckert, and A. Zarras, "Hybroid: Toward android malware detection and categorization with program code and network traffic," in *International conference on information security*, 2021: Springer, pp. 259-278.

[60] M. R. Manesh, J. Kenney, W. C. Hu, V. K. Devabhaktuni, and N. Kaabouch, "Detection of GPS spoofing attacks on unmanned aerial systems," in *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2019: IEEE, pp. 1-6.

[61] M. Sun, Y. Qin, J. Bao, and X. Yu, "GPS Spoofing Detection Based on Decision Fusion with a K-out-of-N Rule," *International Journal of Network Security*, vol. 19, no. 5, pp. 670-674, 2017.

[62] K. Xiao, J. Zhao, Y. He, C. Li, and W. Cheng, "Abnormal behavior detection scheme of UAV using recurrent neural networks," *IEEE Access*, vol. 7, pp. 110293-110305, 2019.

[63] S. C. Bose, "GPS spoofing detection by neural network machine learning," *IEEE Aerospace and Electronic Systems Magazine*, vol. 37, no. 6, pp. 18-31, 2021.

[64] E. Shafiee, M. R. Mosavi, and M. Moazedi, "Detection of spoofing attack using machine learning based on multi-layer neural network in single-frequency GPS receivers," *The Journal of Navigation*, vol. 71, no. 1, pp. 169-188, 2018.

[65] P. Jiang, H. Wu, and C. Xin, "DeepPOSE: Detecting GPS spoofing attack via deep recurrent neural network," *Digital Communications and Networks*, vol. 8, no. 5, pp. 791-803, 2022.

[66] Y.-H. Sung, S.-J. Park, D.-Y. Kim, and S. Kim, "GPS spoofing detection method for small UAVs using 1D convolution neural network," *Sensors*, vol. 22, no. 23, p. 9412, 2022.

[67] J. Campos *et al.*, "A machine learning based smartphone app for gps spoofing detection," in *International Conference on Security and Privacy in Communication Systems*, 2020: Springer, pp. 235-241.

[68] M. Strohmeier, V. Lenders, and I. Martinovic, "Lightweight location verification in air traffic surveillance networks," in *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, 2015, pp. 49-60.

[69] Z. Feng, C. K. Seow, and Q. Cao, "GNSS anti-spoofing detection based on gaussian mixture model machine learning," in *2022 IEEE 25th international conference on intelligent transportation systems (ITSC)*, 2022: IEEE, pp. 3334-3339.

[70] J. Hardy *et al.*, "Unmanned aerial vehicle relative navigation in GPS denied environments," in *2016 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, 2016: IEEE, pp. 344-352.

[71] X. Han *et al.*, "ADS-lead: Lifelong anomaly detection in autonomous driving systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 1, pp. 1039-1051, 2022.

[72] F. Van Wyk, Y. Wang, A. Khojandi, and N. Masoud, "Real-time sensor anomaly detection and identification in automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 3, pp. 1264-1276, 2019.

[73] J. Whelan, T. Sangarapillai, O. Minawi, A. Almehmadi, and K. El-Khatib, "Novelty-based intrusion detection of sensor attacks on unmanned aerial vehicles," in *Proceedings of the*

16th ACM symposium on QoS and security for wireless and mobile networks, 2020, pp. 23-28.

[74] J. Whelan, A. Almehmadi, and K. El-Khatib, "Artificial intelligence for intrusion detection systems in unmanned aerial vehicles," *Computers and Electrical Engineering*, vol. 99, p. 107784, 2022.

[75] A. Xue, F. Xu, J. Xu, J. H. Chow, S. Leng, and T. Bi, "Online pattern recognition and data correction of PMU data under GPS spoofing attack," *Journal of Modern Power Systems and Clean Energy*, vol. 8, no. 6, pp. 1240-1249, 2020.

[76] X. Han *et al.*, "A unified anomaly detection methodology for lane-following of autonomous driving systems," in *2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*, 2021: IEEE, pp. 836-844.

[77] E. Basan, A. Basan, A. Nekrasov, C. Fidge, N. Sushkin, and O. Peskova, "GPS-spoofing attack detection technology for UAVs based on Kullback–Leibler divergence," *Drones*, vol. 6, no. 1, p. 8, 2021.

[78] T. Behdadnia and G. Deconinck, "Anomaly Detection in Automatic Generation Control Systems Based on Traffic Pattern Analysis and Deep Transfer Learning," *arXiv preprint arXiv:2209.08099*, 2022.

[79] D. Sharma, S. K. Gupta, A. Rashid, S. Gupta, M. Rashid, and A. Srivastava, "A novel approach for securing data against intrusion attacks in unmanned aerial vehicles integrated heterogeneous network using functional encryption technique," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 7, p. e4114, 2021.

[80] M. Babaghayou, N. Labraoui, A. A. A. Ari, N. Lagraa, M. A. Ferrag, and L. Maglaras, "SAMA: Security-aware monitoring approach for location abusing and UAV GPS-spoofing attacks on Internet of Vehicles," in *International Conference on Cognitive Radio Oriented Wireless Networks*, 2021: Springer, pp. 343-360.

[81] L. Chaari, S. Chahbani, and J. Rezgui, "Vulnerabilities assessment for unmanned aerial vehicles communication systems," in *2020 international symposium on networks, computers and communications (ISNCC)*, 2020: IEEE, pp. 1-6.

[82] M. Umar, J. Wang, L. Liu, Z. Guo, and S. Wang, "Physical layer authentication in the internet of vehicles based on signal propagation attribute prediction," *Journal of Networking and Network Applications*, vol. 3, no. 1, pp. 1-10, 2023.

[83] K. N. Qureshi, M. A. S. Sandila, I. T. Javed, T. Margaria, and L. Aslam, "Authentication scheme for unmanned aerial vehicles based internet of vehicles networks," *Egyptian Informatics Journal*, vol. 23, no. 1, pp. 83-93, 2022.

[84] D. Yang, Y. Zhao, Z. Yi, D. Yang, and S. He, "A Design Scheme of Data Security for Unmanned Aerial Vehicles," in *International Conference on Advanced Hybrid Information Processing*, 2022: Springer, pp. 165-178.

[85] A. Jain, J. Singh, S. Kumar, Ț. Florin-Emilian, M. Traian Candin, and P. Chithaluru, "Improved recurrent neural network schema for validating digital signatures in VANET," *Mathematics*, vol. 10, no. 20, p. 3895, 2022.

[86] S. Wang, J. Wang, C. Su, and X. Ma, "Intelligent detection algorithm against uavs' gps spoofing attack," in *2020 IEEE 26th international conference on parallel and distributed systems (iCPADS)*, 2020: IEEE, pp. 382-389.

[87] S. Dasgupta, M. Rahman, M. Islam, and M. Chowdhury, "A sensor fusion-based GNSS spoofing attack detection framework for autonomous vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 12, pp. 23559-23572, 2022.

[88] J. García, J. M. Molina, and J. Trincado, "Real evaluation for designing sensor fusion in UAV platforms," *Information Fusion*, vol. 63, pp. 136-152, 2020.

[89] M. Kamal, A. Barua, C. Vitale, C. Laoudias, and G. Ellinas, "GPS location spoofing attack detection for enhancing the security of autonomous vehicles," in *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*, 2021: IEEE, pp. 1-7.

[90] K. Taha, P. D. Yoo, C. Yeun, and A. Taha, "Text classification: A review, empirical, and experimental evaluation," *arXiv preprint arXiv:2401.12982*, 2024.

[91] S. E. Meheretu, S. Y. Hailesilassie, and E. Nigussie, "GNSS-Independent Navigation of UAV through Utilization of Sensor Fusion and Intelligence System," in *2022 International Conference on Information and Communication Technology for Development for Africa (ICT4DA)*, 2022: IEEE, pp. 181-186.

[92] M. Panoff, R. G. Dutta, Y. Hu, K. Yang, and Y. Jin, "On sensor security in the era of IoT and CPS," *SN Computer Science*, vol. 2, no. 1, p. 51, 2021.

[93] S. M. Albrektsen, T. H. Bryne, and T. A. Johansen, "Robust and secure UAV navigation using GNSS, phased-array radio system and inertial sensor fusion," in *2018 IEEE Conference on Control Technology and Applications (CCTA)*, 2018: IEEE, pp. 1338-1345.

[94] M. C. Ang, A. Aghamohammadi, K. W. Ng, E. Sundararajan, M. Mogharrebi, and T. L. Lim, "MULTI-CORE FRAMEWORKS INVESTIGATION ON A REAL-TIME OBJECT TRACKING APPLICATION," *Journal of Theoretical &*

Applied Information Technology, vol. 70, no. 1, 2014.

[95] X. Zhao and Y. Wang, "Machine Learning-Based Analysis of Research Policy Impacts on Academic Performance Metrics," *Informatica,* vol. 49, no. 19, 2025.

[96] M. Ang, E. Sundararajan, K. Ng, A. Aghamohammadi, and T. Lim, "Investigation of threading building blocks framework on real time visual object tracking algorithm," *Applied Mechanics and Materials,* vol. 666, pp. 240-244, 2014.

[97] U. A. Bukar, M. S. Sayeed, S. F. A. Razak, S. Yogarayan, and O. A. Amodu, "An exploratory bibliometric analysis of the literature on the age of information-aware unmanned aerial vehicles aided communication," *Informatica,* vol. 47, no. 7, 2023.