IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 2, 2020, accepted January 27, 2020, date of publication February 13, 2020, date of current version November 23, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.2973759

GNSS Vulnerabilities and Existing Solutions: A Review of the Literature

JASMINE ZIDAN[1], ELIJAH I. ADEGOKE[1], ERIK KAMPERT[1], STEWART A. BIRRELL[1], COL R. FORD[2], AND MATTHEW D. HIGGINS[1], (Senior Member, IEEE)

[1]WMG, The University of Warwick, Coventry CV4 7AL, U.K.
[2]Spirent Communications Plc., Paignton TQ4 7QR, U.K.

Corresponding author: Jasmine Zidan (j.zidan@warwick.ac.uk)

This work was sponsored in part by the Innovate UK through the ELWAG Project under Grant 95143-564624, and in part by the PNTAE project under Grant 133896. The work of Jasmine Zidan was supported by Spirent Communications Plc. as part of the Warwick Collaborative Postgraduate Research Scholarships (WCPRS).

ABSTRACT This literature review paper focuses on existing vulnerabilities associated with global navigation satellite systems (GNSSs). With respect to the civilian/non encrypted GNSSs, they are employed for proving positioning, navigation and timing (PNT) solutions across a wide range of industries. Some of these include electric power grids, stock exchange systems, cellular communications, agriculture, unmanned aerial systems and intelligent transportation systems. In this survey paper, physical degradations, existing threats and solutions adopted in academia and industry are presented. In regards to GNSS threats, jamming and spoofing attacks as well as detection techniques adopted in the literature are surveyed and summarized. Also discussed are multipath propagation in GNSS and non line-of-sight (NLoS) detection techniques. The review also identifies and discusses open research areas and techniques which can be investigated for the purpose of enhancing the robustness of GNSS.

INDEX TERMS GNSS, GNSS vulnerabilities, GNSS robustness, positioning, navigation, timing.

I. INTRODUCTION

Global navigation satellite system (GNSS) is a satellite-based positioning, navigation and timing (PNT). Currently, numerous GNSSs are at various stages of deployment and operational capacity. The American led global positioning system (GPS) is arguably the most well-known and often synonymously interchanged with GNSS in terminology due to its established usage in the market. Nonetheless, it sits alongside the European led GALILEO, Russian led GLONASS, Chinese led BeiDou, Indian led INRSS and the Japanese led QZSS [1]. As a collective framework, GNSS has established itself as a globally dominant and cost effective technology for outdoor PNT [2]. Most GNSSs (GPS, GLONASS and BeiDou) are designed to provide two services: one is free of charge for civil, commercial, and scientific use while the other is restricted for military and government use only [3]. In its current state, GALILEO provides free services only for civilians. By 2020, GALILEO will reach its full capacity by offering four services across both the civilian and military sectors. These services are known as: Open Service, High Accuracy Service, Public Regulated Service and Research and Rescue service [2]. By introducing authentication to the Open and High Accuracy service, significant value will be added to the downstream market via new applications [4].

Recently, there has been growing interest in adopting automation in transportation networks, one of which is connected autonomous vehicles (CAVs) operating within an intelligent transportation system (ITS) [5], [6]. Although there has been significant developments in autonomous driving technologies, the state-of-the art is still inadequate for fully driverless operations [6]. The main challenge of adopting CAVs relates to the ability of obtaining accurate position and timing information for critical applications. For example, in cooperative positioning, precise timing is required for range-based vehicle and infrastructure localization [7]. In addition, accurate positioning information is required for lane detection, route guidance, collision avoidance and emergency response [8]–[12]. With respect to other ITS related applications, GNSS can be adopted in driver assistance applications such as route planning, accident black spot warning as well traffic flow monitoring systems. Data obtained from GNSS can also be fused with complimentary sensor data for active control and passive safety systems, vehicle platooning,

The associate editor coordinating the review of this manuscript and approving it for publication was Venkata Ratnam Devanaboyina.

driver monitoring, pre-crash restrain and collision avoidance systems.

In urban environments GNSS signals suffer from signal blockage which results into multipath propagation and reduced positioning accuracy. Moreover, known vulnerabilities of civilian GNSS to an attacker can render the service unusable for genuine users as seen in denial-of-service (DoS) attacks. By augmenting GNSS with other localization techniques (such as RADAR or inertial sensors), it is possible to mitigate some of these effects [10], [12].

This paper is organized as follows. In Section II, the operating principles of GNSS and an overview of existing vulnerabilities is presented. Sections III and IV discuss physical degradations that occur in GNSS and their solutions. In Sections V and VI, unintentional and international GNSS threats as well as solutions adopted in the literature are presented. The review paper is concluded in Section VII which also highlights areas for future work.

II. THE OPERATING PRINCIPLE, PERFORMANCE CRITERIA AND VULNERABILITIES OF GNSS

A GNSS-constellation consists of three segments: space, ground, and user device [13]. The space segment is composed of a number of satellites within a constellation. The ground station is responsible of synchronizing the satellite's clock to the coordinated universal time (UTC) [14]. The network's ground stations also monitor the performance and health of the satellites and adjust their orbits when required. In addition, ground stations are responsible for uploading data onto satellites which can be used to resolve anomalous situations such as ionospheric delays [14], [15].

Code division multiple access (CDMA) is used by all GNSS constellations except GLONASS in which frequency division multiple access (FDMA) is adopted [16], [17]. In CDMA-based GNSS, the signals are modulated by a unique pseudorandom noise (PRN) code and each satellite uses a different PRN code. This enables the receiver to identify and track unique satellite signals which share the same frequency/channel [18]. In FDMA-based GNSS, each satellite transmits on a different frequency with the same PRN code used by all the satellites within the constellation [17]. An overview of a subset of the existing GNSS constellations' status, number of satellites as well as their access techniques is presented in Table 1. In order to transmit the satellite navigation messages through the radio frequency spectrum, GNSS coded signals are modulated using binary phase shift keying (BPSK) and variations of binary offset carrier (BOC) [18], [19]. The modulated navigation message contains the location of the satellite (ephemeris data), transmission time, and other information that can be used to calculate the time and position of the user device [20].

A. GNSS OPERATING PROCESS

This subsection provides a basic description of how a GNSS receiver calculates its position and timing information, with particular focus on GPS as an example of GNSS.

TABLE 1. A subset of GNSS constellations.

System	Owner	Number	Status	Access technique
GPS	USA	32	Fully operational	CDMA
GLONASS	Russia	26	23 Fully operational, 1 in preparation, 1 on maintenance and 1 on test	FDMA
GALILEO	EU	26	22 fully operational, planned to reach 30 by 2020	CDMA
BeiDou	China	14	14 Fully operational, planned to reach 35 by 2020	CDMA

GPS satellites use three RF links in the L band spectrum (L1, L2 and L5) to transmit GNSS signals. The signals transmitted are made up of a RF carrier, data waveform and spreading code/PRN. In the case of GPS L1 Course Acquisition (C/A), which is also called clear access code (C/A), the PRN code is repeated every 1ms and has a pattern of 1023 bits with an autocorrelation property that allows the receiver to track the received signal [21].

The operating process of a GPS signal reception is in three stages, which are referred to as: acquisition, tracking & correlation and decoding the navigation message [22]). During the acquisition phase, the receiver searches for satellites in view. It then obtains an estimation of the time of arrival (ToA) for each of the available satellites and an estimation of the carrier phase to initiate the tracking [22].

In order to acquire a signal, the receiver generates a local replica of the transmitted code block and attempts to align it with that obtained from the satellite [23]. When the replica aligns with the actual incoming signal into the antenna, the correlation is at its peak [24], [25]. The goal of the correlation process is that the receiver obtains the ToA, carrier phase and an estimate of the pseudorange measurement for each of the received signals [24]. In the code tracking phase, a tracking lock loop is implemented to further align the local replica with the code in the received signal. The code tracking loop correlates the incoming signal with three replica codes of the transmitted code block: Early (E), Prompt (P) and Late (L) with a half chip phase differences between E, P and L [26] (as depicted in Fig.1). Once alignment is achieved, the navigation message is decoded. At this phase, the receiver demodulates the encoded signals and obtains the ephemeris and clock correction information [23]. Given that the ToA in the receiver is measured using a different and less accurate clock, a timing error results from the radio-based distance estimation [10], [27]. This timing error is referred to as the clock bias (δt). The pseudorange to each satellite (shown in (1), where (x, y, z) are the user coordinates to be determined, (x^k, y^k, z^k) are the coordinates of the k^{th} satellite and δb is the clock bias (in meters) is solved iteratively in order to obtain the user's coordinates and clock bias.

$$\rho^k = \sqrt{(x^k - x)^2 + (y^k - y)^2 + (z^k - z)^2 + \delta b} \qquad (1)$$

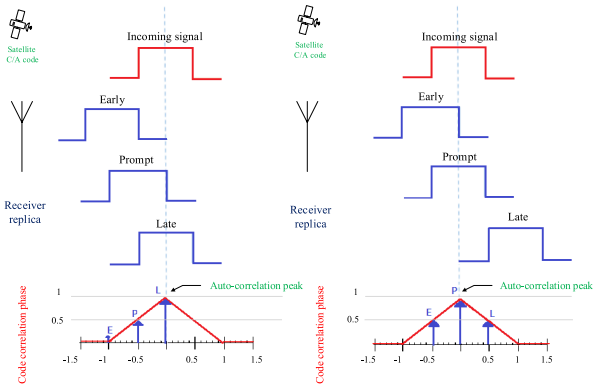


FIGURE 1. Receiver correlation process (adapted from [28]).

This receiver design is adopted to mitigate the effect of the received signal power in the GPS receiver, given that the signals arriving at the receiver on earth are in the range of picowatts [25].

B. PERFORMANCE CRITERIA FOR GNSS NAVIGATION

The performance of a GNSS can be described by the accuracy, integrity, continuity and availability [3], [29] of the signal. These criteria are inherited from the required navigation performance (RNP) concept and they are discussed as follows:

- Accuracy is the degree of congruence of an estimated user position/velocity when compared with the true value [12]. Accuracy is a critical performance measure in precise timing and synchronization applications. Examples are financial transactions timestamp and timing for telecommunications in rail applications [4].
- Integrity is a measure that characterizes the level of correctness of the information supplied by the navigation system. It can be viewed as an indicator of the trust which a user can have in the provided information [30]. Integrity as a GNSS performance feature is applied to the protection level and the associated integrity risk [31]. These two quantities are correlated with the value of the pseudorange measurement delivered at each epoch [32]. Moreover, integrity denotes the ability of a system to provide the user with timely warnings when the navigation system results are inaccurate [11], [33]. This parameter is usually reported as *alert limit* (AL), *integrity risk* (IR), *time to alert* (TTA) and *protection level* (PL).
- Continuity in GNSS applications refers to a reliable operation whereby the system operates without failure for a given period of time [34]. Thus, continuity provides an estimation of the probability that the navigation system fails during an operation given that the system was available from the start of that phase of operation. Continuity builds upon both integrity and accuracy, hence it describes the probability of having a reliable operation over a specified period [30]. This concept is essential in location-based services (LBS) applications as well as railway signaling and rail control [29], [35].
- Availability generally represents the percentage of time in which the navigation system is usable. For specific road applications, GNSS availability is defined as the percentage of the measurement epochs where the terminal delivers the considered output with the required performance irrespective of signal quality [35], [36].

In addition, the geometry of satellites in view also affects the performance of a GNSS. The dilution of precision (DoP) characterizes the position of the user and the distribution of the satellites in view [37]. In a scenario where the satellites are clustered close in the sky, the value of DoP increases and performance is impaired [38]. Increased accuracy can be obtained when the satellites are spread and physically distant from each other [39].

Given that GNSS use cases have different performance requirements, the performance criteria will depend on each particular scenario. In ITS, accuracy is generally expected to be within 1-20m. For urban GNSS applications, robustness to spoofing and jamming, as well as indoor penetration are considered as performance features for GNSSs [13], [40].

C. CURRENT AND FUTURE GNSS VULNERABILITIES

Although GNSS is now widely used and providing positioning, timing and navigating services with an acceptable high level of accuracy in open sky areas, the situation is different for challenging environments such as urban canyons [13], [41]. Due to RF propagation effects, GNSS signals are vulnerable to specific threats such as ionospheric delays and RF interference phenomena [35], [42], [43]. Some GNSS performance challenges exist even prior to signal transmission, for example clock errors and signal modulation faults [44]. GNSS signals can also be affected by space weather as seen in the case of space storms and are exposed to multiple conventional cyber threats [45]. A typical example would be an intruder intercepting a national marine electronics association (NMEA) position report from a receiver and retransmitting it with different coordinates. In this review paper, GNSS vulnerabilities are discussed as physical degradations, and intentional & unintentional threats.

III. PHYSICAL DEGRADATIONS IN GNSS

Due to electromagnetic (EM) wave propagation characteristics, EM waves passing through the earth's atmosphere are affected in many ways [46]. While GNSS signal travel through the wireless channel, the ionosphere introduces frequency dependent delays in the transmitted signal [47], [48]. Ionospheric scintillation causes fading and scattering in the signal which may result in loss of the signal power [49]. The strength of the scintillation is dependent on the solar cycle, space weather and the change of seasons [47], [48], [50], and can virtually be eliminated by applying mathematical calculations in a dual frequency receiver [51].

Buildings in dense urban environments affect the accuracy obtainable from GNSS positioning and timing data

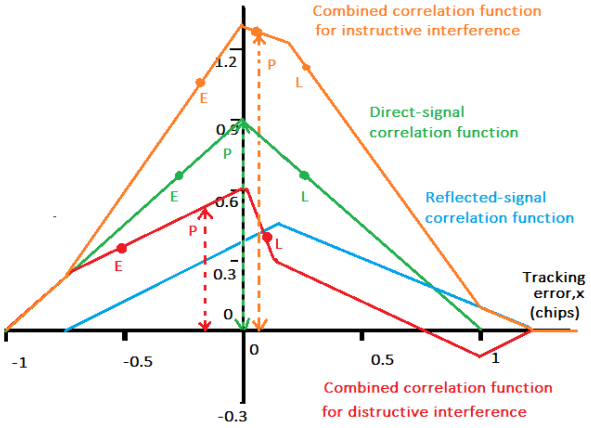


FIGURE 2. The effect of multipath interference on correlation function (adapted from [55]).

in three well known scenarios [52]. In the first scenario, the signals are totally blocked and unavailable for navigation use [53]. A second scenario arises when the signals are received via a reflected path due to the blockage of the line-of-sight (LoS). This phenomenon is known as non line-of-sight (NLoS) reception and the path delays could introduce localization errors as much as 10m [54]. In the third scenario, both LoS and NLoS signals reach the receiver and multipath interference occurs. In most applications and environments, multipath and NLoS effects are considered to be the main physical degradations for GNSS receivers [55]. With respect to the physical degradations, multipath/NLoS propagation affect the code range, carrier phase, signal to noise ratio (SNR) and polarization of received signals [56]. Consequently, the obtainable accuracy is impaired by different effects in varying magnitudes. Given that the correlation function is essential in estimating the ToA of the received signal, large ranging errors and inaccurate position calculation can result from shifting the correlation function of the receiver [55]. Thus multipath propagation affects the accuracy of the code and carrier phase tracking. The positioning error introduced depends on the strength of the reflected signals, path delay, phase difference and the receiver design [57]. In Fig. 2 the destructive or constructive multipath interference effect on the correlation function is depicted. From this illustration, it can be seen that the placement of the local generated replicas of *P*, *E* and *L* is affected by the multipath signal's time delay relative to the LoS (direct) signal. As the constructive multipath adds to the direct signal, *P* develops a positive timing error. This could be noticed from the sharper peak of the composite correlation function when compared to the correlation function of the direct signal. In contrast, the composite correlation function is pushed downwards when compared to the direct signal function for destructive multipath interference. Consequently a negative timing error is developed by *P* and a shorter range is obtained since the measured ToA is earlier than the direct signal.

A. INCONSISTENT PSEUDORANGE MEASUREMENTS

In GNSS multilateration, the ranging error is equal to the difference between the length of the route taken by the NLoS signal and the blocked route. The reception of a GNSS signal in severe conditions, such as a reflected signal via a skyscraper can result in errors larger than 1 km [58].

B. POLARIZATION CHANGE

Changes in the polarization of GNSS signals are usually as a result of the reflections. While LoS signals received from the GNSS satellites have a right-hand circular polarization (RHCP), most of the NLoS signals either have a left-hand circular polarization (LHCP) or a mixed polarization [59]. In order to reduce the position errors between LHCP and RHCP GNSS antennas, more satellites need to be used in multilateration [60]. From the study carried out in [60], the position error difference between RHCP and LHCP reduced by approximately 95% when the satellites used increased from 4 to 9.

C. C/N_0 FLUCTUATIONS

Changes in the carrier to noise ratio (C/N_o) of received GNSS signals in dense urban areas as a result of multipath could either be constructive or destructive. While the constructive multipath causes an increase in the C/N_o, destructive multipath results in signal degradation [55].

IV. SOLUTIONS TO PHYSICAL DEGRADATIONS IN GNSS

In aviation and transport networks where timing and positioning solutions are critical, parallel GNSSs are used to provide the receiver with signal measurement error correction and information about the GNSS performance characteristics [61]. Regional satellite-based augmentation systems (SBAS) such as the European geostationary navigation overlay service (EGNOS) and the wide area augmentation system (WAAS) can be used to enhance GNSS performance [9], [62]. Differential corrections and integrity messages are usually calculated at a central computing center and the corrections are then transmitted using geostationary satellites covering a specific geographical area [63]. In GNSS applications that require precise positioning, mitigating ionospheric scintillation is critical [48], [50]. Its effect on GNSS receivers may be the loss of signal lock by the carrier and code phase tracking loops [48]. A number of methods have been proposed in the literature to compensate for the delays caused by the ionosphere layer. Some of these include computerized ionospheric tomography (CIT), iterative algorithms, non-iterative algorithms and data assimilation techniques [64]–[67].

The scintillation degradation on a GNSS receiver's performance depends on the number of visible satellites for a selected GNSS [47]. Thus, the use of a multi-constellation receiver could increase the total number of visible satellites. In [50], the authors investigated ionospheric scintillation characteristics across the L1, L2 and L5 frequency bands.

The results suggested that dual and multi-frequency devices can be used to estimate and compensate the delays caused by the ionosphere. A similar method was adopted in [68] to mitigate the effect of ionospheric delays. The result showed that for low power devices, the combination of L1 and L2C was optimal and L1 + L5 was suitable for devices without power constraints. The modified receiver also included a Doppler-aided two-frequency signal tracking unit. The troposphere (which is the lowest layer of the atmosphere) also has an influence on the radio signal propagation. The delay introduced by the troposphere is related to the local temperature, relative humidity and pressure. Although this delay is frequency independent and negligible in navigation satellites, it can be compensated for in the receiver [69].

In the literature multipath and NLoS effects are usually investigated simultaneously. Nonetheless, they introduce different effects and should be studied individually. In the literature, three widely known techniques have been adopted in mitigating these effects [70], [71]:

- Antenna based techniques
- Receiver based techniques
- Navigation processor based techniques

A. ANTENNA BASED TECHNIQUES

The authors in [2], [72] suggested that irrespective of the resonating frequencies, the design of an antenna's gain pattern plays a vital role in its immunity to interference.

More recently, the use of multiple input multiple output (MIMO) antennas as a countermeasure for interference has been investigated. By using adaptive antennas, the antenna gain and pattern can be improved and it can be also used for direction of arrival (DoA) measurements. With this direction finding feature, the antenna system can determine the direction of the target and interfering signals [73]. However, in addition to the antenna design, adaptive techniques require the operation of an additional RF signal processing chain.

Given that LoS GNSS signals are RHCP, three techniques (in increasing complexity) were proposed for multipath detection/mitigation in [74] using a dual-polarization antenna. These are: measurement weighting, range-domain multipath correction and tracking domain multipath correction. These techniques are essentially based on implementing individual correlators for the RHCP and LHCP signal as well as measuring the respective (C/N_o). The measurement weighting method was implemented as a weighted-least-square algorithm based on the satellite elevation in [59]; where the Horizontal (*Hor*), North (*N*), East (*E*) and Height (*Hi*) are location attributes for a test point. The multipath mitigating method significantly reduced the average positioning error by 110%, 79%, 151% and 74% for *Hor*, *N*, *E* and *Hi*. A measurement weighting method was presented in [75] where a dual polarized antenna was used to determine the exclusion threshold and weighting for a real time kinematic (RTK) phase-based system. The positioning setup used was based on the Septentrio AsteRx-U dual antenna multi-frequency receiver where only signals from the RHCP antenna port were tracked. Since the LHCP signals require a higher C/N_o in order to be tracked, the local code and timing information obtained from the RHCP signals were replicated for the LHCP correlator. The positioning solution improved the root mean square (RMS) 3D error by: 3% in a static-foliage scenario, 50% in a static-urban scenario and 11% for a dynamic recording from a moving vehicle.

While these techniques are more efficient when they are used in large antenna structures at a higher cost, they become unsuitable for most of the applications that require smaller and cost effective antennas. Miniaturization techniques such as folding the antenna wire also can be used to reduce the antenna dimensions. However, these techniques could alter the return loss and reduce the antenna bandwidth [2].

B. RECEIVER BASED TECHNIQUES

In receiver based techniques, the design of the receiver is modified in order to increase the code discrimination resolution. This results in reducing the code tracking errors (caused by multipath interference within the wireless medium) and path delays [76]. As a result, receiver based signal processing techniques work by separating the direct and reflected signal within the receiver. In other words, they can only mitigate multipath signals and detect NLoS [53]. One of the important measures that is often adopted in assessing the robustness of a GNSS receiver to interference is the C/N_o [38]. In addition, this parameter can be used to assess out-of-band (OOB) interference and low performing satellites [54], [59], [71], [77].

Frequency diversity or multi-GNSS receivers can be used to enhance localization accuracy. From a multi-GNSS constellation approach, [78] adopted a stochastic weighting/exclusion function as well as combining GPS + Galileo signals. Unlike constant (C/N_o) based weighting in [59], a stochastic weighting function was adopted. The positioning solution presented was made up of a code-minus-carrier (CMC) multipath correction module, a pseudorange differencing function for multipath detection and a stochastic-based weighting function. In computing the navigation solution, the positioning framework used all the signals available with iterative de-weighting applied when required. The iterative weighting function used was based on the value of the calculated horizontal DoP (HDoP) at each epoch. In order to enhance the positioning framework, height-constrained environments together with GPS + Galileo signals were added to the framework. From the static field tests carried out, the solution presented in this work was able to improve the horizontal RMS error by 10 - 60%.

Since it is possible that the phase lag resulting from reflections can be relatively constant in a dual-frequency receiver, it is expected that the SNR difference remains constant even in the presence of multipath. In order to increase the multipath detection probability, the use of a three-frequency receiver was investigated in [71]. In this work SNR differences across

three frequencies were modelled into a threshold for determining the presence of multipath. The accuracy of the detector was evaluated using multipath observables (MP1, MP2, MP51). The authors in [79] also adopted a linear combination from a triple frequency receiver to reduce the multipath estimation error associated with dual frequency receivers.

At baseband processing level, the resolution of the code discriminator can be improved for the purpose of estimating the delay. Some implementations in the literature include the delay lock loop (DLL), early-minus-late (EML) correlators, double-delta, strobe correlators, narrow correlators as well as maximum likelihood estimators [80]. These techniques are known to be effective in short/weak multipath scenarios. However, they underperform in severe multipath conditions [81] and also introduce large bias when the LoS signal is weak. Moreover, they are less effective in mitigation carrier phase errors [82].

Another receiver based multipath/NLoS mitigation technique adopted in the literature is vector tracking (VT) [83]. Rather than using separate DLLs to track the PRN of the satellites independently, VT processes the channels together by using an extended Kalman filter (EKF) for tracking as well as user position calculation [76], [83], [84]. In [84], this technique was implemented using a software defined receiver. The VT setup presented used an EKF as a navigation processor, replaced individual DLLs with a vector DLL (VDLL) and a frequency lock loop (FLL) was used for carrier frequency tracking. An adaptive algorithm was also introduced to tune the noise covariance matrix for the EKF and NLoS signals were simulated using LoS echoes. The outcome of the preliminary experiments carried out showed that the VT technique implemented was able to indicate the presence of multipath from the measurement noise. In addition, it was also able to detect the injection of NLoS. The VT setup was adopted in [76] and tested for long NLoS path delay and its sensitivity to a strobe correlator. The effect of NLoS signals was evaluated via simulations with the discriminator output evaluated against a threshold. For a 2 seconds simulated NLoS reception, the VT + (NLoS detection) technique reduced the upper bound of the localization error (RMSE) from 27m to 5m when compared with conventional tracking (CT) and vector tracking. Prior to the simulated NLoS signals, the upper bound of the localization error was approximately 5m for all three methods (VT, CT, VT + NLoS detection). The authors also carried out experiments with a vehicle in a multipath/NLoS environment. The proposed VT technique reduced the mean position error from 30.20 m to 9.51 m when compared with a single-epoch positioning system. The mean error was further reduced to 8.66 m by replacing the early and late correlators of the (receiver used) with a strobe correlator.

An adaptive equalization technique was adopted in [81]. The multipath mitigation framework was made up of a neural network/support vector machine (NN/SVM) based pattern recognition for multipath environment identification and motion classification. A stochastic-gradient-based adaptive filter was also included for multipath compensation. The classifier was evaluated using simulated channel models which contain multipath components of a Galileo signal. For most of the multipath environments investigated, the results showed that the NN outperformed SVM except in a suburban-vehicular environment. The adaptive filter adopted was used to compensate for the multipath induced distortion in the autocorrelation sequence by tuning the filter coefficients for the estimated autocorrelation function. In order to reduce computational complexity, discrete wavelet transform (DWT) was used to equalize the channel impulse response (CIR). In comparison to a fixed strategy such as least mean squares (LMS), recursive least squares (RLS) or wavelet-based RLS, the adaptive filter framework with NN introduced 35% reduction in up-component RMSE.

C. NAVIGATION PROCESSOR BASED TECHNIQUES

At the navigation processor, a consistency check can be applied to pseudorange measurements for the purpose of enhancing the localization accuracy. With this method, the pseudorange residual (test statistic) is evaluated against a chi-squared threshold to determine the possible presence of NLoS or multipath signals. This same principle is applied in receiver autonomous integrity monitoring (RAIM) [23], [85], [86]. This multipath mitigation method is implemented as a fault detection exclusion (FDE) algorithm whereby ''faulty'' signals are detected and excluded based on the ability of the receiver to obtain a group of self-consistent measurements [86]. A FDE method was evaluated in [86] using two algorithms: Greedy and Exhaustive. The former excludes SV signals successively while the later finds a group of consistent measurements. This work adopted a C/N_o based weighting and a chi-square test was used to determine the threshold. The positioning framework was tested for trajectories in Tokyo, Japan with open-sky, sub-urban, middle-urban and deep urban environments and was combined with DGNSS for correction. For all the trajectories considered, Greedy and Exhaustive FDE were able to introduce a 29% and 31% decrease in the mean positioning error. In deep urban environment, the Exhaustive FDE was able reduce the positioning error by 8%. While the consistency check was able to find a group of consistent measurements, the positioning solution was erroneous due to NLoS and multipath signals.

3D mapping of buildings has also been adopted in the literature for mitigating physical degradations in GNSS. The ability of 3D models to predict satellite visibility was investigated in [41]. In most implementations, 3D mapping is used to improve localization accuracy through shadow matching, terrain height-aiding or NLoS detection [87]. In [52], a position-domain integration of shadow matching and 3D mapping were used to improve horizontal accuracy in a dense urban area. The framework calculated position information using both methods and evaluated two weighting strategies for combination. The first method weights the solution according to the covariances while the other weights based on the assumption that one method is better suited

for across-street directions. The covariance based weighting was able to reduce the RMS horizontal error from 25.9 m to 6.1 m. The work in [52] was extended in [53] by using a hypothesis-domain integration as well as evaluating Galileo signals. By initializing the likelihood-based 3D mapping aided (LB-3DMA) and shadow matching with a least squares 3DMA ranging algorithm, the search areas were significantly reduced. In the LB-3DMA framework, satellite visibility was predicted and a likelihood score was associated with the position solutions obtained from the measurements and the error covariance. The shadow matching technique also predicts satellite visibility using boundaries from the 3D map. A score was associated to the position solutions obtained based on the error between the prediction and the C/N_o of the satellites measured. In order to null false hypothesis, joint ranging was obtained by multiplying the likelihood from both methods. Within an urban/dense area, the proposed framework was able to reduce the localization error from 24.4 m to 3.4 m. With regards to a 2-constellation setup, negligible improvement was observed. This was associated with the severe NLoS signals that impair the performance of shadow matching.

For maximum reliability across a range of different challenging environments, advanced GNSS receivers should be integrated with other navigation and positioning technologies such as inertial navigation systems (INS) [88], [89]. In scenarios where there is a prolonged GNSS outage or NLoS signal propagation, GNSS/INS fusion can be used to improve the positioning accuracy. In order to compensate for multipath and NLoS effects in urban canyons, [90] used an adaptive fuzzy unscented Kalman filter (AF-UKF) to fuse INS from a gyroscope and accelerometers with a dual constellation (GPS + BeiDou) GNSS receiver. By implementing thresholds for satellite elevation angle, C/N_o, some NLoS/multipath GNSS signals were excluded. The fussy calibration logic implemented was based on the azimuth difference between the received satellite and the ego vehicle, elevation angle as well as the C/N_o. The framework was tested in Nanjing, China which has typical urban propagation features. In a dense area with high rise buildings, the AF-UFF framework was able to provide 81% improvement to a EKF based solution and 75% to a UKF only solution. However, the limitations of this proposed solution is that under certain conditions, the position accuracy might be degraded to some extent. This is related to the observation noise covariance, whereby healthy satellite signals that seem unhealthy would be largely amplified.

In [91], Consistency check and double difference were used to mitigate physical degradation in GNSS pseudorange and vehicle-to-vehicle (V2V) ranging. Consistency check was individually applied to GNSS pseudorange and the V2V ranging. The outputs were then fed into a cooperative positioning (CP) algorithm that computes the absolute and relative position of all the participating vehicles. From the measurement results obtained from u-blox M8T receivers, the weighted cooperative algorithm was able to reduce the mean positioning error from 17.71 m to 5.33 m when compared to a LS iterative CP algorithm. While this framework introduced significant improvements, the framework was not evaluated in a dense urban environment.

Contrary to explicit methods such as V2V ranging, [92] proposed an implicit cooperative positioning technique that uses vehicle-to-features (V2F), V2V and GNSS ranging for cooperative vehicle positioning. The physical features adopted in this work are inactive cars, traffic lights and pedestrians. The dynamic model was used to model the states of the vehicle and a first order Markov model for non-cooperative features. In a distributed architecture, a consensus based Gaussian message passing (GMP) algorithm was used for estimating posterior probabilities for cooperative and non-cooperative objects. For a simulated trajectory with rural and urban regions, the positioning technique was able to reduce the localization error from 4.5m to less than 1m (200 non-cooperative features). In a more realistic setup with mobile pedestrians and severely degraded GNSS signals, the framework reduced the upper bound of the localization error from 40m to sub-meter accuracy. The results also showed that increasing the number of participating vehicles reduced the localization error. However, the improvement introduced is negligible when the number of features is high.

Sparse estimation was adopted in [93] as a means of mitigating multipath. This theory was adopted based on the assumption that: multipath signals can be modelled as additive biases, most satellites in view are not affected and that the measurement equation is linear with respect to the state vector. Assuming a sparse vector representing pseudorange and pseudorange rate errors, the method solved a modified version of the LASSO problem with a weighting function that is dependent on the C/N_o and satellite elevation. The framework was evaluated against synthetic, real data as well as data obtained from a typical outdoor scene. In comparison with an EKF implementation from [94], the framework reduced the upper bound horizontal and vertical RMS localization error from 64.67 m to 47.22 m and 4.92 m to 3.43 m. In an urban environment, the median horizontal error of the proposed method was 0.04 m. With respect to the limitations of the theory, the authors discovered that framework performance degrades when the number of biased satellite channels exceeds 5.

D. REMARKS ON MITIGATING GNSS PHYSICAL DEGRADATION

While significant mitigating techniques have been presented in academia, original equipment manufacturers (OEMs) for GNSS receivers have also adopted these multipath mitigating techniques:

1) The Zephyr geodetic antenna from Trimble Navigation which uses a n-point antenna feed to improve the RHCP characteristics of the antenna. This in turn increases the receiver's ability to reject multipath signals [96]. Other commercially available antennas such as the NovAtel GPS Antenna [97] reject LHCP signals.

2) APME+ used in AsteRx-m2 Septentrio receivers. This is implemented using additional correlators as posterior multipath estimators for code and phase measurements [98]. A similar method using a dedicated phase correlator has also been patented by Leica Geosystems [99].
3) The use of phased arrays and digital signal processing as seen in NAVSYS high-gain advanced GPS receiver (HAGR). This system creates a composite signal from a 16-element array which can create nulls in specified directions [95]. The test results carried out by NAVSYS showed that the HAGR P(Y) code beam steering system increased the averaged C/N_o for the SVs tracked by approximately 10 dB when compared to multipath rejection antennas from [97]. In addition, the HAGR attenuated the multipath signal powers by an additional 10 dB.
4) Fence Antenna Technology and the Advanced Multipath Reduction (AMR) from Topcon Positioning Systems Inc. Both patented techniques are used to filter out multipath errors as well as reject multipath on both code and carrier phase measurements [100].
5) The Q-lock algorithm from GeoMax. This algorithm is designed to detect correction services for the purpose of multipath mitigation [101].

In general, the ability to detect multipath/NLoS signals provides a means for a system designer to either exclude these signals or mitigate their effects in computing the position solution of the receiver. The choice of the approach or the resulting performance depends on several factors such as the signal quality from other satellites, length of multipath delay, signal-type modulation, code chipping rate, pre-correlation bandwidth, number of multipath signals, relative power of multipath signals, correlator chip spacing as well as the code/carrier tracking algorithm [71], [102]. In Table 2, a summary of the techniques discussed is presented. Since some of the surveyed literature adopt multiple solutions, some of the works appear under multiple methods.

V. INTENTIONAL AND UNINTENTIONAL THREATS TO GNSS

Given that GNSS signals received by users on the earth's surface have an extremely low signal strength, they are susceptible to RF interference which can result in a direct impact on the performance of the navigation system [44], [46]. These interference sources could either be unintentional or intentional [2], [46], [103]. Unintentional interferences sources such as multipath and other RF propagation mechanisms are usually associated with the physical characteristics of the radio signals. On the other hand, intentional interferences targeted at ''blinding'' the receiver's antenna with noise are referred to as jamming [104]. They can affect geo-location technologies by either degrading the receiver performance or by causing a DoS [103], [105]. Moreover, interferences from other radio standards such as digital enhanced cordless telecommunication (DECT) could also blind or degrade the performance of a GNSS receiver [106].

Jamming could also be unintentional. An example of this could be the use of a personal privacy device (PPD). In most scenarios, a PPD transmits a carrier at a desired frequency to prevent a nearby GNSS receiver from functioning [107]. However, rogue devices could be used to misguide a user device by transmitting false GNSS-like signals. This act is known as spoofing and it's more dangerous than jamming as it is not always detected [108], [109]. Spoofing attacks are generally divided into two main categories: replay attacks (meaconing) and forged signal attacks [2], [109], [110].

VI. SOLUTIONS TO GNSS INTENTIONAL AND UNINTENTIONAL THREATS

According to [111], most of the countermeasures for GNSS threats can be classified under one of the following categories:

- Encryption mechanisms
- Codeless-cross-correlation measures
- Signal statistic analyzing methods
- Antenna based

A. ENCRYPTION MECHANISMS

This technique relies on the encryption algorithms for restricting access to the signal. Encryption mechanisms usually involve some sort of communication security (COMSEC) and navigation message (NAVSEC) measures [112]. They are generally complex and expensive which makes them impractical for most end user applications [113]. However, they are used in the GPS military signal communications. With GALILEO, an affordable authentication service known as open service-navigation message authentication (OS-NMA) will be used by authorized user devices that are capable of interpreting encrypted signals [2]. This service will only be available to a selected number of authorities including the European Commission and the European External Action Service [34]. With an embedded authentication layer, it is envisaged that GALILEO will provide improved positioning accuracy and signal robustness [4], [114].

B. CODELESS-CROSS-CORRELATION MEASURES

In [115]–[117], the use of correlations between unknown encrypted GPS L1 P(Y) code signals from two receivers was used to detect spoofing. While these represented initial implementations, [118] presented a cohesive explanation and demonstration of the proposed concept. Since there are known signal relationships between the known carrier & code phase of the C(A) code with the encrypted P(Y) code, part of the encrypted signals at two receivers were correlated for spoofing detection. The technique is premised on the hypothesis that if a PRN is spoofed, the cross-correlation statistic will be low. The signals used to test the algorithm were obtained from commercial of-the-shelf (COTS) devices, while the software processing was evaluated offline.

TABLE 2. Summary of solutions to GNSS physical degradation.

Method (Reference)	Features	Performance	Cost
	Antenna based		
Dual polarization antennas [59], [75]	Individual front end for RHCP and LHCP signals Individual correlators for RHCP and LHCP signal processing C/N_o thresholds adopted for multipath-environment classification Mitigation implemented as weighting, range or tracking correction	Positioning error improved significantly by 110% (*Hor*), 79% (*N*), 151% (*E*) and 74% (*Hi*) [59] RMS 3D error reduction: 3% Static-foliage, 50% Static-urban, 11% Dynamic [75]	High
Dual constellation [78] adopted in [90], [91]	GPS L2, Galileo E5b Pseudorange differencing	Horizontal RMS error improved by 10 - 60%	High
Phased array antenna [95]	16-element antenna array 6 processing channels for signal processing Programmable DSP with adaptive beam and null-forming	10 dB C/N_0 gain +10 dB multipath power rejection	High
	Receiver based		
Stochastic weighting [78]	(CMC) multipath error correction Height constraints, Pseudorange differencing, Dual GNSS	Horizontal RMS error improved by 10 - 60%	High
Frequency diversity receivers [71], [79]	Threshold based detection SNR differencing and Code minus carrier Evaluation of multipath variables (MP1,MP2 MP51)	Variation in test statistic shown to infer multipath	Med
Pattern recognition & Stochastic-gradient-based filtering [81]	Neural Network, SVM environment classification Adaptive filter (Equalization) Wavelet-based LMS (W-LMS) & Wavelet-based RLS (W-RLS)	35% RMSE improvement (up-component)	Med
Vector Tracking NLoS [76], [84]	EKF with adaptive noise covariance Strobe correlator Early-Minus-Late delay lock loop (EML-DLL)	28.5% improvement (Mean error)	Med
	Navigation processor based		
3D Mapping 3DMA + Shadow matching[52]	Terrain height aiding, Position-domain integration Use of building boundaries 3D Maps for satellite visibility, Consistency checks	76% improvement in RMS horizontal accuracy	Med
3D Mapping 3DMA + Shadow matching[53] Consistency check [86] adopted in [52], [53], [91]	Terrain height aiding, Hypothesis-domain integration Use of building boundaries, Galileo signals 3D Maps for satellite visibility, Consistency checks Greedy & Exhaustive FDE C/N_o -based weighting, chi-square threshold	86% improvement 3-constellation 86% improvement 2-constellation (RMS horizontal accuracy) 29% and 31% improvement for Greedy and Exhaustive FDE (mean error) 8% in deep urban (Exhaustive FDE)	Med Low
Data fusion [90]	UKF, RISS, Fuzzy Logic, Dual constellation receiver Satellite elevation and C/N_o thresholds for NLoS/Multipath detection/exclusion	81% improvement to EKF, 75% improvement to UKF (Euclidean error)	Med
Cooperative positioning [91] [92]	Consistency check, Double difference GPS, BeiDou Implicit CP, GMP, Belief propagation Kalman filter vehicle tracking	107% improvement to LS (Mean error) Peak improvement of 175% (200 static features) Upper bound error reduced from 40 m to sub meter (Urban canyon) (RMSE)	Med High
Sparse estimation [93]	C/N_o & Satellite elevation based weighting EKF, l_1 regularization	upper bound RMSE reduced from 64.67 m to 47.22 m (Horizontal); 106.10 m to 44.72 m (Vertical)	Med

An estimate of the detection statistic was obtained from a quadrature baseband mixing of the P(Y) code and an inter-receiver time mapping was implemented to align the C/A code start/stop times. From the experimental results presented, this framework was able to detect a spoofed PRN. With respect to the performance of the setup, the authors noted that for receivers placed in the same location experienced cross-talk between channels. This was associated with the Doppler shifts and code delays of other GPS signals.

The framework presented in [11] extends the dual receiver P(Y)-code correlation concept to an *ad hoc* network of cooperative receivers referred to as ''cross-check receivers''. A 2-stage authentication process was adopted in this work: a pair-wise check (which involves a P(Y) correlation) and decision aggregation where pair-wise checks are combined and evaluated. Three system architectures were evaluated numerically in this work. In the first architecture, the user and cross-check receivers collect in phase-quadrature (IQ) signals for a specific PRN and the user sends a snippet of the signal acquired to cross-check receivers. The cross-check receivers correlate the signals and send a decision to the user. The user then performs decision aggregation and determines if it has been spoofed or not. In the second, the user performs both correlation and decision aggregation. Consequently introducing additional delay. This method allows the user to exclude malicious cross-check receivers and also minimize radio transmissions. In the third, a third party server collects these signals and performs both correlation and decision making tasks. Given that the remote server (or third party) has more computing resources, this approach is fast, scalable and can

also be used for position/time assertion. From the numerical analysis carried out, the authors showed that:

- An increased number of cross-check receivers increases performance.
- For a fixed probability of false alarm, probability of missed detection decreases exponentially with increasing number of cross-check receivers.

With respect to the pair-wise checks, the authors also carried out measurements in 1) an urban location characterized with low SNR and low satellite visibility (3 satellites visible) 2) an open space characterized with high SNR and high satellite visibility (10 satellites in view). At the urban location, two static receivers were 3000 km apart and the authentication framework was able to detect spoofed signals as the test statistic was less than the specified threshold. For the open space scenario, the mobile receivers were spaced 22 km apart. The framework was able to detect spoofing, however, the test statistic dropped rather slowly.

C. SIGNAL STATISTIC ANALYZING METHODS

This approach either implements consistency checks or a statistical tests on features such as automatic gain control (AGC), clock error, signal quality, signal power, propagation delay and the angle of arrival (AoA) [119], [120].

By observing the discrepancies between the GPS and free-INS position solution, a tightly coupled residual RAIM GPS-INS system was presented in [121] for detecting spoofed GPS signals. In contrast to the typical RAIM based platforms where redundancy is via multiple satellites, a gyroscope + accelerometer based INS was used to provide redundant measurement variables. The authors noted that for improved performance, it is essential to regularly calibrate the system due to diverging covariance errors of the inertial sensors. The framework was evaluated by determining a worst case spoofing scenario that maximizes the IR for 8 minutes and the simulated use case was a precision landing phase for an aircraft. From the results presented, if the spoofer has substantial knowledge of the user's trajectory, the framework could not detect an attack.

The authors in [108] presented structural power analysis (SPA) as part of a spoofing detection method (SPM). The SPM was made up of an AGC monitoring unit, a SPA unit and an acquisition level detection unit. Within the SPA unit, spoofed PRNs are detected prior to despreading by inspecting the power spectral content. After passing through the SPA unit, spoofing can also be detected at the acquisition level block by either using a cross-ambiguity function (CAF) that evaluates correlation peaks or by detecting anomalies in the total number of correlation peaks.

In [122], the authors discussed the use of absolute power monitoring techniques to reduce the effect of a spoofing attack. The study first illustrates that a C/N_o discrimination method is not an effective spoofing countermeasure when it is used alone. The authors showed that if the receiver is able to detect changes in the noise floor, this enhanced capability can be combined with C/N_o discrimination to detect spoofed PRNs. A similar technique that characterises the noise floor is presented in [44]. The method presented is quite robust provided that the code phase difference between the authentic and spoofed PRNs is > 1.5 chips. The technique referred to as the total signal energy measurement (TSEM) method was shown to outperform the SPA implementation in [123]. The authors evaluated the technique via simulation for four different scenarios with equal number of spoofed and authentic PRNs. For a scenario whereby the spoofing received power increases over time, the TSEM method could detect the spoofed signals when the spoofing power exceeded the receive power of authentic signals. In the presence of multipath signals, the simulation result showed significant variations in the test statistic. While it was noted that this could result in higher false alarm rate, this drawback can be mitigated by combining the TSEM with a multipath rejecting antenna or a suitable mitigating technique presented in Section IV.

With respect to analyzing the clock error, [124] presented a spoofing detecting solution that correlated the clock bias with the receiver motion. With this approach, spoofing was detected if there was a deviation between the position-velocity-time (PVT) solution and the prediction. The accuracy of this approach was reported to vary with the receiver's trajectory, clock stability and the estimated parameters for the clock model.

Signal quality monitoring (SQM) can also be used for detecting spoofed signals [125], [126]. This technique is based on Neyman Pearson (NP) detection theory. The NP theorem is adopted in GNSS signal processing to identify distortions in the correlation peak. By evaluating a metric or a combination of metrics (which characterize the signal quality) against a predefined threshold, this technique can be used to detect spoofed GNSS signals [125], [127]. In the literature, two metrics have been widely adopted for SQM, these are the Delta test metric and the Ratio test metric [128]. The early-late phase (ELP) metric has also been proposed in [129]. Given that the GNSS receiver is able to estimate the statistics of the metrics prior to the attack, two Ratio test metrics were used in [125] alongside an additional correlator. The proposed SQM framework was evaluated for a real case scenario from [130]:-Scenario 6. The authors showed that a single SQM metric was not sufficient in detecting a spoofed signal since the effects of the spoofer occurs at slightly different time slots for the individual metrics adopted. By observing the detection ratio of both metrics, the authors showed that the metrics adopted in the framework were able to track the spoofed signals. Furthermore, the results showed that the metrics selected had different characteristics and a joint detection approach was suggested. Since these SQM metrics are generally complementary [125], [127], a multi-metric joint detection SQM technique (based on the ELP + Delta and ELP + Ratio test metrics) was presented in [127]. The authors evaluated two metric combination strategies: the Amplitude combination (AmpM) and the

TABLE 3. Summary of solutions to GNSS intentional and unintentional threats.

Reference	Method/Features	Complexity	Cost
	Encryption Mechanism		
[112]–[114]	Provides improved positioning accuracy and security. Involves COMSEC and NAVSEC measures (OS-NMA) authentication service is an application of these techniques.	High	High
	Codeless-cross-correlation Measures		
[11]	Cross-correlation of P(Y) from user and *ad hoc* cross-check receivers Cross-check receivers could be unreliable Third party position assertion, Hypothesis testing	Med	Med
[115]–[118]	Cross-correlation of P(Y) from reference and test receiver Susceptible to meaconing and cross-talk	High	Med
	Signal statistic analyzing methods		
[44]	Noise floor estimation Requires code phase difference > 1.5 chips Requires additional multipath mitigation technique	Med	Med
[108]	SPA inspects the power spectral content prior to despreading	Low	Med
[121]	Tightly coupled INS-RAIM, Redundancy provided by multiple satellites, gyroscope and accelerometer Regular system calibration required	Med	Med
[122]	Absolute noise floor power monitoring, C/N_o discrimination	Low	Med
[124]	Clock error analysis combined with receiver motion. Provides reliable results in multipath environments	Med	Med
[125]	Signal quality monitoring using two ratio metrics. Ratio metrics based on early, late, extra-early, extra-late and prompt correlators	Med	High
[127]	Joint SQM metrics based on ELP and Ratio/Delta metric. Two metric combination methods presented.	Med	Med
[130]	Attained 100% detection rate for Scenario 2 and 3		
[131]	so-called symmetric difference metric Bayesian M-ary hypothesis testing. Interference power advantage, interference-to-authentic code and carrier offsets extracted from model	Med	Med
[132]	Kalman filter innovation for ramp-type faults Two averaging techniques adopted for a time window. chi-square based test statistic	Med	Med
	Antenna based methods		
[46]	Beam former points the antenna beam towards desired satellites. Multi-antenna combined with INS and RISS	High	High
[133]	Inter-antenna vector from a 2-antenna system and DoA used for detection	High	High
[134]	Single antenna combined with RISS	Low	Low
[135]	Beam former used to send null towards the spoofer	High	High
[136]	Deep nulls generated towards the spoofer & jammer Does not require receiver hardware modifications Assumes spoofing signals from the same direction Orthogonal complement subspace adopted for jamming suppression	Medium	Low

Probability of false alarm combination (PfaM), with the simulation results showing that the PfaM had a better performance with respect to spoofing detection. The simulated results showed that individual SQM metrics (Delta, Ratio and ELP) attained similar probability of detection. With the ELP combined with either metrics using the PfaM combination, a 20% improvement was introduced in the detection ratio. The authors also evaluated the framework ([130] Scenario 2 & Scenario 3). In both scenarios, the Pfa (ELP + Ratio) attained a 100% detection rate during the spoofed signal window. The SQM techniques discussed in this subsection are typically limited by the fact that multipath can also cause distortions in the correlation function peak. As such, spoofing detected using this technique could be as a result of multipath delay of the received signals.

With respect to classifying multipath, spoofing and jamming, [131] implemented a power-distortion detector that attained a false alarm rate of less than 0.6%. The detection statistic in [131] was based on the received power and symmetric difference measurements. The receive power measurements are premised on the fact that interference in the bandwidth of the RF front end will cause distinguishable variations in the received power. While other events can also cause power variations, the authors combined this with the so-called symmetric difference metric since it is easy to implement. A Bayesian M-ary hypothesis testing framework was adopted for classifying the absence or presence of interfering signals: multipath, spoofing and jamming. The interference detector was evaluated against real GNSS data for spoofing, multipath and jamming. The performance of the

TABLE 4. Impact of GNSS vulnerabilities on performance criteria.

GNSS vulnerability	Accuracy	Integrity	Availability	Continuity
A)- Physical degradation				
• Ionospheric delays	Med	Med	Med	Med
• Clock errors	Low	Low	Low	Low
• Signal modulation faults	Low	Low	Low	Low
• Space weather	Low	Low	Low	Low
Multipath	High	High	High	Med
NLoS	High	Med	High	High
B)- Unintentional & intentional threats				
ine Interference with other communication systems	Med	Med	Med	Med
Jamming	-	-	High	High
Spoofing	High	High	-	-

detector showed that all occurrences of spoofing or jamming were detected. For a severe case where the spoofed signal controls the interference-to-authentic carrier phase offset and executes a nulling-and-replacement attack, the detector classified spoofing as jamming for over 90% of time.

Similar to FDE techniques adopted in GNSS physical degradation, [132] recently adopted a loosely coupled INS + GNSS framework (based on Kalman filter innovation) for spoofing detection. For a given time window, the authors evaluated two averaging methods: innovation averaging whereby by the normalized sum-squared innovations at each epoch is averaged or the measurement averaging whereby averaging is done within the whole time window followed by a snapshot. The performance of the spoofing detection presented was compared with traditional snapshot methods and the results showed that the framework (innovation or measurement) performed better in detecting ramp-type spoofing profiles with low drift magnitude (< 0.5 m/s). With respect to low drift spoofing profiles, the authors showed that the measurement averaging technique slightly outperformed the innovation method since it is less affected by spoofing attacks with a long measurement update cycles.

D. ANTENNA BASED METHODS

A single antenna GNSS receiver integrated with a reduced inertial sensor system (RISS) was presented in [134] for robust navigation. Although the positioning accuracy was improved by the RISS, the performance degraded when exposed to jamming or spoofing signals. This framework was extended in [46] by integrating it with an antenna array. The result showed that the array provided better estimation of the spoofing signal DoA when compared with a single GPS antenna. Moreover, the framework presented was able to detect and mitigate spoofing signals. The enhancement offered through multiple antennas is attainable since the signals impinging on an array have spatial features which can be manipulated to mitigate spoofing from an EM propagation point of view [136].

With respect to multi antenna strategies, a two-antenna spoofing detection system was developed in [133]. The approach adopted relied on the difference between the DoA of the authentic and spoofed signals. The positioning setup was tested under various spoofing attacks with varying transmit power at different locations. While the test results showed that the navigation system detected more spoofing signals when compared to RAIM, it requires an advanced phase-locked loop (PLL) to track the carrier phase. The concept of transmitting null signals from a digital beam former has also been reported in the literature [135]. By using correlators and matrix processing to the array outputs, synthetic nulls can be created in the direction of the spoofer.

An array method was also proposed in [136] for simultaneously suppressing spoofing and jamming signals. The framework presented was made up of a jamming suppression unit (JSU), spoofing suppression unit (SSU) and a useful signal enhancement unit (UEU) connected in tandem. Since jamming involves signals with higher power, all the signals from the array are fed into a JSU prior to spoofing processing. Three scenarios involving spoofing/jamming signals were investigated in this work. In order to evaluate the performance, the authors compared the array gain with [137] and [138]. The summary of the results presented showed that the proposed method was able to generate deep null beams towards jamming and spoofing signals as well as enhance the array gain towards authentic signals. While the array method presented showed promising results, it is based on the assumption that the spoofed signals/PRNs are from the same direction.

In Table 3, a summary of the literature discussed in this section is presented. It is noteworthy that spoofing attacks are dynamic and there are no spoofing countermeasure techniques that are able to work in all scenarios. Consequently, it is essential that the end user considers the cost, complexity and other factors based on a given use case scenario [44].

VII. CONCLUSION

This paper has presented an overview of GNSS vulnerabilities and the current solutions adopted in the literature for the purpose of increasing the performance and robustness of a GNSS receiver. From the surveyed literature, it is evident that physical degradation severely affects the localization figure of merit. With respect to intentional threats, jamming attacks can be easily carried out, while spoofing requires sophisticated techniques to avoid detection. This is because

the attack requires precise positioning information of the target device. Moreover, the spoofer needs to adapt it signal strength and maintain a LoS to the target device. This scenario is quite challenging for moving targets. In Table 4, an impact summary is presented. This table quantifies the possible effects the surveyed vulnerabilities have on the respective GNSS performance criteria.

From the surveyed literature, it is evident that a combination of techniques will be required to mitigate different physical and logical vulnerabilities present in GNSS. Moreover, with the growth of automotive internet of things (IoT) and increased wireless network penetration, radio access technologies such as Wi-Fi can be used to enhance localization in urban areas. As shown in surveyed works in [139], this technology is now gradually being adopted in GNSS receiver design. Furthermore, with advances in computing, more machine learning/artificial intelligence techniques will be adopted in addressing these GNSS vulnerabilities. In regards to future research directions, the authors believe the following areas can be further investigated for GNSS robustness.

1) Hybrid GNSS: By combining different GNSS interference countermeasures (such as ray-tracing, consistency checks), multipath and NLoS effects can be mitigated and the accuracy of the positioning solution can be enhanced.
2) Multi-constellation receivers: Advanced signal processing techniques can be adopted in multi-constellations GNSS receivers. These techniques can also be combined with other interference countermeasure to improve localization availability and accuracy.
3) GNSS/INS fusion: Positioning and localization accuracy can be enhanced by adopting advanced data sensor fusion methods especially in limited GNSS coverage areas. Further work is required in analyzing INS measurement error sources as these affect the performances of fusion framework. GNSS/INS fusion can also be used for spoofing detection. However, more studies are required in reducing the complexity of these techniques.
4) Cooperative positioning: This technique can be combined with consistency checks in reducing the localization errors obtained from GNSS receivers in urban environments.
5) Multi- radio network: With respect to GNSS physical degradation, multi radio access technologies can be adopted to improve localization accuracy. With the evolution of mobile/terrestrial communications, technologies such as Wi-Fi, 5G millimeter wave and algorithms such as antenna beam steering/forming can be adopted in urban/built environments.

REFERENCES

[1] A. Santra, S. Mahato, S. Mandal, S. Dan, P. Verma, P. Banerjee, and A. Bose, "Augmentation of GNSS utility by IRNSS/NavIC constellation over the Indian region," *Adv. Space Res.*, vol. 63, no. 9, pp. 2995–3008, 2018, doi: 10.1016/j.asr.2018.04.020.
[2] "GNSS user technology report," Eur. GNSS Agency, Prague, Czech Republic, Tech. Rep. 1, 2016. [Online]. Available: https://bit.ly/2e32Y7u
[3] C. J. Hegarty and E. Chatre, "Evolution of the global navigation satelliteSystem (GNSS)," *Proc. IEEE*, vol. 96, no. 12, pp. 1902–1917, Dec. 2008.
[4] "GNSS market report," Eur. GNSS Agency (GSA), Prague, Czech Republic, Tech. Rep. 5, 2017. [Online]. Available: https://www.gsa.europa.eu/system/files/reports/gnss_mr_2017.pd
[5] T. Frey, "Driverless highways: Creating cars that talk to the roads," *J. Environ. Health*, vol. 75, no. 5, pp. 38–40, 2012.
[6] F. O. Flemisch, K. Bengler, H. Bubb, H. Winner, and R. Bruder, "Towards cooperative guidance and control of highly automated vehicles: H-mode and conduct-by-wire," *Ergonomics*, vol. 57, no. 3, pp. 343–360, Mar. 2014.
[7] M. Tahir, S. S. Afzal, M. S. Chughtai, and K. Ali, "On the accuracy of inter-vehicular range measurements using GNSS observables in a cooperative framework," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 682–691, Feb. 2019.
[8] Z. Tian, Y. Cai, S. Huang, F. Hu, Y. Li, and M. Cen, "Vehicle tracking system for intelligent and connected vehicle based on radar and V2V fusion," in *Proc. Chin. Control Decis. Conf. (CCDC)*, Jun. 2018, pp. 6598–6603. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8408291
[9] *Satellite-Derived Time and Position: A Study of Critical Dependencies*, Government Office for Science, London, U.K., 2018, pp. 1–86. [Online]. Available: https://bit.ly/2NtRcj4
[10] U. Lee, J. Jung, S. Jung, and D. H. Shim, "Development of a self-driving car that can handle the adverse weather," *Int. J. Automot. Technol.*, vol. 19, no. 1, pp. 191–197, Feb. 2018.
[11] L. Heng, D. B. Work, and G. X. Gao, "GPS signal authentication from cooperative peers," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 4, pp. 1794–1805, Aug. 2015.
[12] A. Mukhtar, L. Xia, and T. B. Tang, "Vehicle detection techniques for collision avoidance systems: A review," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 5, pp. 2318–2338, Oct. 2015.
[13] R. T. Ioannides, T. Pany, and G. Gibbons, "Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques," *Proc. IEEE*, vol. 104, no. 6, pp. 1174–1194, Jun. 2016.
[14] H. G. Berns and R. J. Wilkes, "GPS time synchronization system for K2K," in *Proc. IEEE Conf. Real-Time Comput. Appl. Nucl. Part. Plasma Phys. 11th IEEE NPSS Real Time Conf. Conf. Rec.*, Jun. 1999, vol. 47, no. 2, pp. 480–483. [Online]. Available: https://ieeexplore.ieee.org/document/846177/
[15] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance*, 2nd ed., M. Lincoln, Ed. Massachusetts, CA, USA: Ganga-Jamuna Press, 2011.
[16] J.-B. Kim, D. S. Park, J. M. Ahn, K.-J. Kim, and K.-W. Song, "A study of CSS based GNSS spreading modulation technique," in *Proc. 18th Asia–Pacific Conf. Commun. (APCC)*, Jeju Island, South Korea, Oct. 2012, pp. 208–209. [Online]. Available: https://ieeexplore.ieee.org/document/6388132/
[17] G. R. Lennen, "The USSR's Glonass P-code-Determination and initial results," in *Proc. 2nd Int. Tech. Meeting Satell. Division Inst. Navigat.*, Colorado Spring, Co, USA, 1989, pp. 77–83. [Online]. Available: https://www.ion.org/publications/abstract.cfm?articleID=11836
[18] S. Tabibi, F. Geremia-Nievinski, and T. V. Dam, "Statistical comparison and combination of GPS, GLONASS, and multi-GNSS multipath reflectometry applied to snow depth retrieval," *IEEE Trans. Geosci. Remote Sens.*, vol. 55, no. 7, pp. 3773–3785, Jul. 2017. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7894171
[19] F. D. Nunes, F. M. G. Sousa, and J. M. N. Leitao, "Gating functions for multipath mitigation in GNSS BOC signals," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 43, no. 3, pp. 951–964, Jul. 2007.
[20] W. Lechner and S. Baumann, "Global navigation satellite systems," *Comput. Electron. Agricult.*, vol. 25, nos. 1–2, pp. 67–85, 2000.
[21] J. W. Betz, "SATNAV signals," in *Engineering Satellite-Based Navigation and Timing: Global Navigation Satellite Systems, Signals, and Receivers*. Hoboken, NJ, USA: Wiley, 2015, ch. 3, pp. 37–99.
[22] J. W. Betz, "Introduction," in *Engineering Satellite-Based Navigation and Timing: Global Navigation Satellite Systems, Signals, and Receivers*. Hoboken, NJ, USA: Wiley, 2015, ch. 1. [Online]. Available: https://media.wiley.com/product_data/excerpt/72/11186159/1118615972.pdf

[23] M. J. Rycroft, *Understanding GPS: Principles and Applications*, 2nd ed., E. D. Kaplan and C. J. Hegarty, Eds. Boston, MA, USA: Artech House, 2006. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1364682697833378

[24] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, and S. H. Jensen, *A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach*. Boston, MA, USA: Springer, 2007.

[25] A. E. Suzer and H. Oktal, "PRN code correlation in GPS receiver," in *Proc. 8th Int. Conf. Recent Adv. Space Technol. (RAST)*, Jun. 2017, pp. 189–193. [Online]. Available: https://ieeexplore.ieee.org/document/8002960/

[26] B. N. Vu and M. Andrle, "The code and carrier tracking loops for GPS signal," in *Proc. 16th Int. Conf. Mechatronics-Mechatronika*, Dec. 2014, pp. 569–574.

[27] Z. Liu, B. Chen, and B. Zhang, "Global navigation satellite systems," in *International Encyclopedia of Geography: People, the Earth, Environment and Technology*. Oxford, U.K.: John, 2017, pp. 1–10 doi.wiley.com/10.1002/9781118786352.wbieg1151.

[28] J. Van Sickle, "GPS and GNSS for geospatial professionals: Tracking loops," Dept. Geography, PennState College Earth Mineral Sci. [Online]. Available: https://www.eeducation.psu.edu/geog862/node/1785

[29] J. Marais, J. Beugin, and M. Berbineau, "A survey of GNSS-based research and developments for the european railway signaling," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2602–2618, Oct. 2017.

[30] N. Zhu, J. Marais, D. Betaille, and M. Berbineau, "GNSS position integrity in urban environments: A review of literature," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 9, pp. 2762–2778, Sep. 2018.

[31] D. Salos, C. Macabiau, A. Martineau, B. Bonhoure, and D. Kubrak, "Analysis of GNSS integrity requirements for road user charging applications," in *Proc. 2010 5th ESA Workshop Satell. Navigat. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, Dec. 2010, pp. 1–8. [Online]. Available: https://hal-enac.archives-ouvertes.fr/hal-01022508%0D.

[32] P.-Y. Gillieron, L. Ruotsalainen, F. Peyret, S. Feng, and J. Engdahl, "The SaPPART cost action: Towards positioning integrity for road transport," in *Proc. Eur. Navigat. Conf. (ENC)*, May 2016.

[33] J. Rife and S. Pullen, "Aviation applications," in *GNSS Applications and Methods*, S. Gleason and E. D. Gebre, Eds. Norwood, MA, USA: Artech House, 2009, ch. 10, pp. 263–286.

[34] "European radio navigation plan," Eur. Commission, Brussels, Belgium, Tech. Rep., 2018. [Online]. Available: https://ec.europa.eu/docsroom/documents/33024

[35] M. Monnerat, "Integrity monitoring for road applications," in *Proc. Positioning Conf. Workshop (CNES CCT PDS, ENAC)*, Toulouse, France, 2013.

[36] D. Margaria, E. Falletti, and T. Acarman, "The need for GNSS position integrity and authentication in ITS: Conceptual and practical limitations in urban contexts," in *Proc. IEEE Intell. Vehicles Symp. Proc.*, Jun. 2014, pp. 1384–1389.

[37] K. Kazmierski, "Performance of absolute real-time multi-GNSS kinematic positioning," *Artif. Satell.*, vol. 53, no. 2, pp. 75–88, Jun. 2018. [Online]. Available: http://content.sciendo.com/view/journals/arsa/53/2/article-p75.xml

[38] O. Elmasry, M. Tamazin, H. Elghamarawy, M. Karaim, A. Noureldin, and M. Khedr, "Examining the benefits of multi-GNSS constellation for the positioning of high dynamics air platforms under jamming conditions," in *Proc. 11th Int. Symp. Mechatronics Appl. (ISMA)*, Mar. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8330133/

[39] R. B. Langley, "Dilution of precision," *GPS World*, vol. 10, no. 5, pp. 52–59, 1999.

[40] X. Meng, S. Roberts, Y. Cui, Y. Gao, Q. Chen, C. Xu, Q. He, S. Sharples, and P. Bhatia, "Required navigation performance for connected and autonomous vehicles: Where are we now and where are we going?" *Transp. Planning Technol.*, vol. 41, no. 1, pp. 104–118, Jan. 2018.

[41] L. Wang, P. D. Groves, and M. K. Ziebart, "Multi-constellation GNSS performance evaluation for urban canyons using large virtual reality city models," *J. Navigat.*, vol. 65, no. 3, pp. 459–476, Jul. 2012.

[42] J. J. Spilker, P. Axelrad, B. W. Parkinson, and P. Enge, "Interference effects and mitigation techniques," in *Global Positioning System: Theory and Applications*, 1st ed. Washington, DC, USA: American Institute of Areonautics and Astronautics, 1996, ch. 20, pp. 717–771.

[43] J. J. Spilker, P. Axelrad, and B. W. Parkinson, "Multipath effects," in *Global Positioning System: Theory and Applications*, 1st ed. Washington, DC, USA: American Institute of Areonautics and Astronautics, 1996, ch. 14, pp. 547–568.

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

[45] N. Can, "Legal issues concerning the cyber security of GNSS," in *Proc. 7th Int. Conf. Recent Adv. Space Technol. (RAST)*, Jun. 2015, pp. 861–864. [Online]. Available: https://ieeexplore.ieee.org/document/7208461/

[46] N. Vagle, A. Broumandan, and G. Lachapelle, "Multi-antenna GNSS and INS/odometer coupling for robust vehicular navigation," ENAC, Toulouse, France, 2017.

[47] V. K. Srinivasu, N. Dashora, D. S. Prasad, K. Niranjan, and S. G. Krishna, "On the occurrence and strength of multi-frequency multi-GNSS Ionospheric Scintillations in Indian sector during declining phase of solar cycle 24," *Adv. Space Res.*, vol. 61, no. 7, pp. 1761–1775, 2018, doi: 10.1016/j.asr.2017.08.036.

[48] N. Hlubek, J. Berdermann, V. Wilken, S. Gewies, N. Jakowski, M. Wassaie, and B. Damtie, "Scintillations of the GPS, GLONASS, and Galileo signals at equatorial latitude," *J. Space Weather Space Climate*, vol. 4, p. A22, 2014. [Online]. Available: http://www.swsc-journal.org/10.1051/swsc/2014020

[49] J. Aarons, "Global morphology of ionospheric scintillations," *Proc. IEEE*, vol. 70, no. 4, pp. 360–378, Apr. 1982. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1456582

[50] C. S. Carrano, K. M. Groves, W. J. McNeil, and P. H. Doherty, "Scintillation characteristics across the GPS frequency band," in *Proc. ION-GNSS*, 2012, pp. 1972–1989 https://gto.bc.edu/pub/user/grovesk/for_altshuler/carrano-ion-2012-final-labeled.pdf

[51] S. Jin and D. Li, "3-D ionospheric tomography from dense GNSS observations based on an improved two-step iterative algorithm," *Adv. Space Res.*, vol. 62, no. 4, pp. 809–820, Aug. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0273117718304460

[52] M. Adjrad and P. D. Groves, "Intelligent urban positioning: Integration of shadow matching with 3D-mapping-aided GNSS ranging," *J. Navigat.*, vol. 71, no. 1, pp. 1–20, Jan. 2018.

[53] M. Adjrad and P. Groves, "3D-mapping-aided GNSS exploiting Galileo for better accuracy in dense urban environments," in *Proc. Eur. Navigat. Conf. (ENC)*, May 2017, pp. 108–118.

[54] L.-T. Hsu, "Analysis and modeling GPS NLOS effect in highly urbanized area," *GPS Solutions*, vol. 22, no. 1, p. 7, Jan. 2018.

[55] P. D. Groves, *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems*, 2nd ed. Norwood, MA, USA: Artech House, 2013.

[56] J. K. Ray, M. E. Cannon, and P. Fenton, "GPS code and carrier multipath mitigation using a multiantenna system," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 37, no. 1, pp. 183–195, Jan. 2001.

[57] Z. Jiang, P. D. Groves, W. Y. Ochieng, S. Feng, C. D. Milner, and P. G. Mattos, "Multi-constellation GNSS multipath mitigation using consistency checking," in *Proc. 24th Int. Meeting Satell. Division Inst. Navigat.*, Portland, OR, USA, 2011, pp. 3889–3902. [Online]. Available: http://discovery.ucl.ac.uk/1349795/1/3889.pdf

[58] G. Castaldo, A. Angrisano, S. Gaglione, and S. Troisi, "P-RANSAC: An integrity monitoring approach for GNSS signal degraded scenario," *Int. J. Navigat. Observ.*, vol. 2014, Sep. 2014, Art. no. 173818, doi: 10.1155/2014/173818.

[59] Z. Jiang and P. D. Groves, "NLOS GPS signal detection using a dual-polarisation antenna," *GPS Solutions*, vol. 18, no. 1, pp. 15–26, Jan. 2014.

[60] R. U. R. Lighari, M. Berg, J. Kallankari, A. Parssinen, and E. T. Salonen, "Analysis of the measured RHCP and LHCP GNSS signals in multi-path environment," in *Proc. Int. Conf. Localization GNSS (ICL-GNSS)*, Jun. 2016, pp. 1–6.

[61] T. Murphy and T. Imrich, "Implementation and operational use of ground-based augmentation systems (GBASs)—A component of the future air traffic management system," *Proc. IEEE*, vol. 96, no. 12, pp. 1936–1957, Dec. 2008. [Online]. Available: https://0-ieeexplore-ieee-org.pugwash.lib.warwick.ac.uk/stamp/stamp.jsp?tp=&arnumber=4745660

[62] T. Dautermann, "Civil air navigation using GNSS enhanced by wide area satellite based augmentation systems," *Prog. Aerosp. Sci.*, vol. 67, pp. 51–62, May 2014.

[63] (2016). *What is SBAS?*. [Online]. Available: https://www.gsa.europa.eu/european-gnss/what-gnss/what-sbas

[64] G. S. Bust and C. N. Mitchell, "History, current state, and future directions of ionospheric imaging," *Rev. Geophys.*, vol. 46, no. 1, pp. 1–23, Feb. 2008.
[65] S. Jin, J. U. Park, J. L. Wang, B. K. Choi, and P. H. Park, "Electron density profiles derived from ground-based GPS observations," *J. Navigat.*, vol. 59, no. 3, pp. 395–401, Sep. 2006.
[66] K. Bhuyan, S. B. Singh, and P. K. Bhuyan, "Application of generalized singular value decomposition to ionospheric tomography," *Ann. Geophys.*, vol. 22, no. 10, pp. 3437–3444, Jun. 2010. [Online]. Available: https://hal.archives-ouvertes.fr/file/index/docid/317677/filename/angeo-22-3437-2004.pdf
[67] M.-R. G. Razin, "Development and analysis of 3D ionosphere modeling using base functions and GPS data over Iran," *Acta Geodaetica et Geophys.*, vol. 51, no. 1, pp. 95–111, 2016. [Online]. Available: https://0-link-springer-com.pugwash.lib.warwick.ac.uk/content/pdf/10.1007%2Fs40328-015-0113-9.pdf
[68] P. Bolla and K. Borre, "Performance analysis of dual-frequency receiver using combinations of GPS L1, L5, and L2 civil signals," *J. Geodesy*, vol. 93, no. 3, pp. 437–447, Mar. 2019.
[69] J. Douša, M. Eliaš, P. Václavovic, K. Eben, and P. Krč, "A two-stage tropospheric correction model combining data from GNSS and numerical weather model," *GPS Solutions*, vol. 22, no. 3, p. 77, 2018, doi: 10.1007/s10291-018-0742-x.
[70] P. D. Groves, Z. Jiang, L. Wang, and M. K. Ziebart, "Intelligent urban positioning using multi-constellation GNSS with 3D mapping and NLOS signal detection," Inst. Navigat., Nashville, TN, USA, 2012, pp. 458–472. [Online]. Available: http://discovery.ucl.ac.uk/1394444/1/0681.pdf
[71] P. R. R. Strode and P. D. Groves, "GNSS multipath detection using three-frequency signal-to-noise measurements," *GPS Solutions*, vol. 20, no. 3, pp. 399–412, 2016. [Online]. Available: https://link.springer.com/content/pdf/10.1007%2Fs10291-015-0449-1.pdf
[72] C. C. Counselman, "Multipath-rejecting GPS antennas," *Proc. IEEE*, vol. 87, no. 1, pp. 86–91, Jan. 1999. [Online]. Available: https://0-ieeexplore-ieee-org.pugwash.lib.warwick.ac.uk/document/736343/
[73] W. Fan, L. Hentila, F. Zhang, P. Kyosti, and G. F. Pedersen, "Virtual drive testing of adaptive antenna systems in dynamic propagation scenarios for vehicle communications," *IEEE Access*, vol. 6, pp. 7829–7838, 2018. [Online]. Available: https://0-ieeexplore-ieee-org.pugwash.lib.warwick.ac.uk/document/8269321/
[74] P. D. Groves, Z. Jiang, B. Skelton, P. A. Cross, L. Lau, Y. Adane, and I. Kale, "Novel multipath mitigation methods using a dual-polarization antenna," Univ. Westminster, Portland, OR, USA, 2010, pp. 140–150.
[75] D. Egea-Roca, A. Tripiana-Caballero, J. A. Lopez-Salcedo, G. Seco-Granados, W. De Wilde, B. Bougard, J.-M. Sleewaegen, and A. Popugaev, "GNSS measurement exclusion and weighting with a dual polarized antenna: The FANTASTIC project," in *Proc. 8th Int. Conf. Localization GNSS (ICL-GNSS)*, Jun. 2018, pp. 1–6.
[76] L.-T. Hsu, S.-S. Jan, P. D. Groves, and N. Kubo, "Multipath mitigation and NLOS detection using vector tracking in urban environments," *GPS Solutions*, vol. 19, no. 2, pp. 249–262, Apr. 2015. [Online]. Available: https://link.springer.com/content/pdf/10.1007%2Fs10291-014-0384-6.pdf
[77] L.-T. Hsu, "GNSS multipath detection using a machine learning approach," in *Proc. IEEE 20th Int. Conf. Intell. Transp. Syst. (ITSC)*, Oct. 2017, pp. 1–6.
[78] A. Pirsiavash, A. Broumandan, G. Lachapelle, and K. OrKeefe, "Detection and De-weighting of multipath-affected measurements in a GPS/Galileo combined solution," in *Proc. Eur. Navigat. Conf. (ENC)*, Apr. 2019, pp. 1–11.
[79] Y. Kamatham and S. S. Vemuri, "Analysis and estimation of multipath interference using dual and triple frequency GNSS signals," in *Proc. IEEE Appl. Electromagn. Conf. (AEMC)*, Dec. 2017, pp. 1–2.
[80] M. Z. H. Bhuiyan and E. S. Lohan, "Multipath mitigation techniques for satellite-based positioning applications," in *Global Navigation Satellite Systems: Signal, Theory and Applications*, S. P. Jin, Ed. Rijeka, Croatia: InTech, 2012, pp. 405–426. [Online]. Available: https://www.intechopen.com/books/global-navigation-satellite-systems-signal-theory-and-applications/multipath-mitigation-techniques-for-satellite-based-positioning-applications
[81] N. Sokhandan, A. Broumandan, and G. Lachapelle, "GNSS multipath mitigation using low complexity adaptive equalization algorithms," in *Proc. 5th ESA Int. Colloq. Sci. Fundam. Aspects Galileo*, Braunschweig, Germany, 2015, pp. 1–9.
[82] X. Chen, F. Dovis, S. Peng, and Y. Morton, "Comparative studies of GPS multipath mitigation methods performance," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 3, pp. 1555–1568, Jul. 2013.
[83] N. Kan, H. Hurskainen, and J. Nurmi, "Vector tracking loop design for degraded signal environment," in *Proc. Ubiquitous Positioning Indoor Navigat. Location Based Service*, Oct. 2010.
[84] L.-T. Hsu, P. Groves, and S.-S. Jan, "Assessment of the multipath mitigation effect of vector tracking in an urban environment," in *Proc. ION Pacific PNT Meeting*, Honolulu, Hawaii, HI, USA, Apr. 2013, pp. 498–509.
[85] P. D. Groves and Z. Jiang, "Height aiding, C/N_0 weighting and consistency checking for GNSS NLOS and multipath mitigation in urban areas," *J. Navigat.*, vol. 66, no. 5, pp. 653–669, 2013. [Online]. Available: http://discovery.ucl.ac.uk/1399116/1/wp4_JoN_2013_v8 with notice.pdf
[86] L.-T. Hsu, H. Tokura, N. Kubo, Y. Gu, and S. Kamijo, "Multiple faulty GNSS measurement exclusion based on consistency check in urban canyons," *IEEE Sensors J.*, vol. 17, no. 6, pp. 1909–1917, Mar. 2017.
[87] M. Adjrad and P. D. Groves, "Enhancing least squares GNSS positioning with 3D mapping without accurate prior knowledge," *J. Inst. Navigat.*, vol. 64, no. 1, pp. 75–91, Mar. 2017.
[88] Y. Chen, S. Zhao, and J. A. Farrell, "Computationally efficient carrier integer ambiguity resolution in multiepoch GPS/INS: A common-position-shift approach," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 5, pp. 1541–1556, Sep. 2016.
[89] M. Wu, J. Ding, L. Zhao, Y. Kang, and Z. Luo, "An adaptive deep-coupled GNSS/INS navigation system with hybrid pre-filter processing," *Meas. Sci. Technol.*, vol. 29, no. 2, Feb. 2018, Art. no. 025103. [Online]. Available: http://iopscience.iop.org/article/10.1088/1361-6501/aa9672/pdf
[90] X. Li, R. Jiang, X. Song, and B. Li, "A tightly coupled positioning solution for land vehicles in urban canyons," *J. Sensors*, vol. 2017, Mar. 2017, Art. no. 5965716.
[91] G. Zhang, W. Wen, and L.-T. Hsu, "A novel GNSS based V2V cooperative localization to exclude multipath effect using consistency checks," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Apr. 2018. pp. 1465–1472. [Online]. Available: https://ieeexplore.ieee.org/document/8373540/
[92] G. Soatti, M. Nicoli, N. Garcia, B. Denis, R. Raulefs, and H. Wymeersch, "Implicit cooperative positioning in vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3964–3980, Dec. 2018.
[93] J. Lesouple, T. Robert, M. Sahmoudi, J.-Y. Tourneret, and W. Vigneau, "Multipath mitigation for GNSS positioning in an urban environment using sparse estimation," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 4, pp. 1316–1328, Apr. 2019.
[94] K. Deergha Rao, M. N. S. Swamy, and E. I. Plotkin, "GPS navigation with increased immunity to modeling errors," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 40, no. 1, pp. 2–11, Jan. 2004.
[95] A. Brown, N. Gerein, N. Corporation, and U. N. Observatory, "Test results from a digital p(y) code beamsteering receiver for multipath minimization," in *Proc. ION 57 th Annu. Meeting*, vol. 2001, pp. 00–14.
[96] E. Krantz, S. Riley, and P. Large, "The design and performance of the Zephyr geodetic antenna," in *Proc. 14th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Jun. 2016, pp. 1942–1951.
[97] (2019). *Gpsantenna Model 501*. [Online]. Available: https://www.novatel.com/assets/Documents/Manuals/om-20000001.pdf
[98] (2019). *Apme+ Principle*. [Online]. Available: https://www.septentrio.com/en/apme-multipath-mitigation-technology
[99] D. Bétaille, J. Maenpa, H. Euler, and P. Cross, "A new approach to GPS phase multipath mitigation," in *Proc. Nat. Tech. Meeting Inst. Navigat.*, Jan. 2003, pp. 243–253. [Online]. Available: https://www.ion.org/publications/abstract.cfm?articleID=3768
[100] (2019). *Technology for GNSS Products*. [Online]. Available: https://www.topconpositioning.com/gb/gnss-network-solutions
[101] (2019). *GNSS*. [Online]. Available: https://geomax-positioning.com/products/gnss
[102] M. Sahmoudi and R. E. Landry, "Multipath mitigation techniques using maximum-likelihood principle," *Inside GNSS*, vol. 3, no. 8, pp. 24–29, 2008. [Online]. Available: https://www.insidegnss.com/auto/novdec08-sahmoudi-v1.pdf
[103] P. Craven, R. Wong, N. Fedora, and P. Crampton, "Studying the effects of interference on GNSS signals," in *Proc. Int. Tech. Meeting The Inst. Navigat.*, San Diego, CA, USA, 2013, pp. 893–900. [Online]. Available: http://www.scopus.com/inward/record.url?eid=2-s2.0-84881134719&partnerID=tZOtx3y1
[104] M. Troglia Gamba, M. D. Truong, B. Motella, E. Falletti, and T. H. Ta, "Hypothesis testing methods to detect spoofing attacks: A test against the TEXBAT datasets," *GPS Solutions*, vol. 21, no. 2, pp. 577–589, Apr. 2017.

[105] Y. Ying, T. Whitworth, and K. Sheridan, "GNSS interference detection with software defined radio," in *Proc. IEEE 1st AESS Eur. Conf. Satell. Telecommun. (ESTEL)*, Oct. 2012. pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/document/6400121/

[106] A. Grant, P. Williams, N. Ward, and S. Basker, "GPS Jamming and the Impact on Maritime Navigation," *J. Navigat.*, vol. 62, no. 2, pp. 173–187, Apr. 2009.

[107] S. Pullen and G. Gao, "GNSS jamming in the name of privacy," *Inside GNSS*, vol. 7, no. 2, pp. 34–43, 2012. [Online]. Available: http://www.insidegnss.com/auto/marapr12-Pullen.pdf

[108] A. Broumandan, A. Jafarnia-Jahromi, and G. Lachapelle, "Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver," *GPS Solutions*, vol. 19, no. 3, pp. 475–487, Jul. 2015. [Online]. Available: http://plan.geomatics.ucalgary.ca/

[109] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7445815

[110] D. Maier, K. Frankl, R. Blum, B. Eissfeller, and T. Pany, "Preliminary assessment on the vulnerability of NMA-based Galileo signals for a special class of record & replay spoofing attacks," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Apr. 2018, pp. 63–71.

[111] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the GNSS spoofing threat and countermeasures," *ACM Comput. Surv.*, vol. 48, no. 4, p. 64:1–64:31, May 2016, doi: 10.1145/2897166.

[112] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 2, pp. 1073–1090, Apr. 2013. [Online]. Available: https://ieeexplore.ieee.org/document/6494400/

[113] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, "A blueprint for civil GPS navigation message authentication," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, May 2014, pp. 262–269. [Online]. Available: https://ieeexplore.ieee.org/document/6851385/

[114] K. Wesson and M. Rothlisberger, "A proposed navigation message authentication implementation for civil GPS anti-spoofing," in *Proc. Ion GNSS*, 2011, pp. 3129–3140.

[115] B. W. O'Hanlon and M. L. Psiaki, "Real-time spoofing detection in a narrow-band civil GPS receiver," in *Proc. Ion GNSS*, 2010, pp. 2211–2220.

[116] B. W. O'Hanlon, M. L. Psiaki, T. E. Humphreys, and J. A. Bhatti, "Real-time spoofing detection using correlation between two civil GPS receivers," in *Proc. ION GNSS Meeting*. Nashville, TN, USA, 2012, pp. 3584–3590.

[117] 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," *J. Inst. Navigat.*, vol. 60, no. 4, pp. 267–278, Dec. 2013.

[118] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "GPS spoofing detection via dual-receiver correlation of military signals," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 4, pp. 2250–2267, Oct. 2013.

[119] P. Y. Hwang and G. A. McGraw, "Receiver Autonomous Signal Authentication (RASA) based on clock stability analysis," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, May 2014, pp. 270–281. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6851386

[120] D. M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)," *J. Inst. Navigat.*, vol. 59, no. 4, pp. 281–290, Dec. 2012. [Online]. Available: https://www.ion.org/publications/abstract.cfm?articleID=102583

[121] S. Khanafseh, N. Roshan, S. Langel, F.-C. Chan, M. Joerger, and B. Pervan, "GPS spoofing detection using RAIM with INS coupling," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, May 2014, pp. 1232–1239.

[122] A. Jafarnia Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements," *Int. J. Satell. Commun. Network.*, vol. 30, no. 4, pp. 181–191, Jul. 2012. [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1002/sat.964/abstract

[123] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "Pre-despreading authenticity verification for GPS L1 C/A signals," *Navigation*, vol. 61, no. 1, pp. 1–11, 2014. [Online]. Available: http://doi.wiley.com/10.1002/navi.50

[124] A. Jafarnia-Jahromi, S. Daneshmand, A. Broumandan, J. Nielsen, and G. Lachapelle, "PVT Solution Authentication Based on Monitoring the Clock State for a Moving GNSS Receiver," in *Proc. Eur. Navigat. Conf. (ENC)*, Vienna, Austria, 2013, pp. 1–11. [Online]. Available: https://schulich.ucalgary.ca/files/plan/jafarniajahromi2013_conference.pdf

[125] K. Ali, E. G. Manfredini, and F. Dovis, "Vestigial signal defense through signal quality monitoring techniques based on joint use of two metrics," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, May 2014, pp. 1240–1247.

[126] E. G. Manfredini, F. Dovis, and B. Motella, "Validation of a signal quality monitoring technique over a set of spoofed scenarios," in *Proc. 7th ESA Workshop Satell. Navigat. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, Dec. 2014, pp. 1–7.

[127] C. Sun, J. W. Cheong, A. G. Dempster, H. Zhao, and W. Feng, "GNSS spoofing detection by means of signal quality monitoring (SQM) metric combinations," *IEEE Access*, vol. 6, pp. 66428–66441, 2018.

[128] R. E. Phelts, "Multicorrelator techniques for robust mitigation of threats to GPS signal quality," Ph.D. dissertation, Stanford Univ., Stanford, CA, USA, 2001.

[129] O. M. Mubarak and A. G. Dempster, "Analysis of early late phase in single-and dual-frequency GPS receivers for multipath detection," *GPS Solutions*, vol. 14, no. 4, pp. 381–388, Sep. 2010. [Online]. Available: https://link.springer.com/content/pdf/10.1007%2Fs10291-010-0162-z.pdf

[130] T. Humphreys, J. Bhatti, D. Shepard, and K. Wesson, "The texas spoofing test battery: Toward a standard for evaluating GPS signal authentication techniques," in *Proc. 25th Int. Tech. Meeting Satellite Division Inst. Navigat. (ION GNSS)*, Nashville, TN, USA, Sep. 2012, pp. 3569–3583.

[131] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS signal authentication via power and distortion monitoring," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 54, no. 2, pp. 739–754, Apr. 2018.

[132] Y. Liu, S. Li, Q. Fu, Z. Liu, and Q. Zhou, "Analysis of kalman filter innovation-based GNSS spoofing detection method for INS/GNSS integrated navigation system," *IEEE Sensors J.*, vol. 19, no. 13, pp. 5167–5178, Jul. 2019.

[133] M. Psiaki, B. O'Hanlon, S. Powell, J. Bhatti, K. Wesson, T. Humphreys, and A. Schofield, "GNSS spoofing detection using two-antenna differential carrier phase," in *Proc. 27th Int. Tech. Meeting Satell. Division Inst. Navigat., ION (GNSS)*, vol. 4, 2014, pp. 2776–2800.

[134] J. Georgy, A. Noureldin, M. J. Korenberg, and M. M. Bayoumi, "Low-cost three-dimensional navigation solution for RISS/GPS integration using mixture particle filter," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 599–615, Feb. 2010.

[135] C. E. McDowell, "GPS spoofer and repeater mitigation system using digital spatial nulling," U.S. Patent 7 250 903, Jul. 31, 2007.

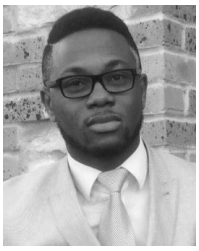
[136] Y. Hu, S. Bian, B. Li, and L. Zhou, "A novel array-based spoofing and jamming suppression method for GNSS receiver," *IEEE Sensors J.*, vol. 18, no. 7, pp. 2952–2958, Apr. 2018.

[137] W. Sun and M. G. Amin, "A self-coherence anti-jamming GPS receiver," *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp. 3910–3915, Oct. 2005.

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

[139] E. I. Adegoke, J. Zidane, E. Kampert, C. R. Ford, S. A. Birrell, and M. D. Higgins, "Infrastructure Wi-Fi for connected autonomous vehicle positioning: A review of the state-of-the-art," *Veh. Commun.*, vol. 20, Dec. 2019, Art. no. 100185. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214209619302323

JASMINE ZIDAN received the B.Sc. degree in communication and electronics engineering and the M.Sc. degree in communication engineering from Tishreen University, Syria, in 2010 and 2015, respectively. She is currently pursuing the Ph.D. degree with WMG, The University of Warwick, U.K. Her recent research is specialized in GNSS robustness for CAVs in urban environments.



ELIJAH I. ADEGOKE received the B.S. degree in electrical and electronics engineering from Covenant University, Nigeria, in 2009, and the M.Sc. degree in mobile communications and the Ph.D. degree in electronic engineering from Loughborough University, in 2013 and 2018, respectively. From 2017 to 2018, he was a Research Associate with the 5GRC, Loughborough University. From 2010 to 2014, he worked as a Network Engineer with telecoms firms in Nigeria and U.K. He is currently a Research Fellow with WMG. His work is focused on Wi-Fi GNSS fusion measurement and modelling for localization in CAVs. His research interests include Wi-Fi based V2X, radio propagation and modelling, Wi-Fi positioning systems, heterogeneous wireless networks, IP mobility, self-organizing networks, sensor fusion, and machine learning for wireless communications.

ERIK KAMPERT received the M.Sc. and Ph.D. degrees in natural sciences from Radboud University Nijmegen, The Netherlands, in 2005 and 2012, respectively. He was with the Molecular Materials Group and the High Field Magnet Laboratory at the Institute for Molecules and Materials, RU. He continued his research as a Postdoctoral Researcher with the Dresden High Magnetic Field Laboratory, Helmholtz-Zentrum Dresden-Rossendorf, Germany, where he conducted electrical transport experiments in pulsed magnetic fields in collaboration with visiting international scientists. In 2017, he joined the Connectivity Group, WMG's Intelligent Vehicles Research Team, University of Warwick, U.K., as a Senior Research Fellow. Using his vast background in RF electromagnetics, the focus of his current research is on 5G millimeter-wave communication for vehicular-to-everything and the Industrial Internet of Things applications.

STEWART A. BIRRELL received the B.Sc. degree (Hons.) in sport science from the University of Hertfordshire and the Ph.D. degree in ergonomics from Loughborough University. As a specialist in human factors, his research is with the interface of design, engineering, technology, and psychology, and focuses on the evaluation of human interaction with vehicle technology. He has worked in both academia and industry with different domains from military applications to transportation. He currently works as an Associate Professor, and Human Factors Capability Lead for the Intelligent Vehicle research group, WMG, University of Warwick. He has almost 100 scientific papers, book sections, articles, or features published to date, and is an Associate Editor of the Q1/4 international IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS.

COL R. FORD received the B.Sc. degree (Hons.) in computer science from the University of Hertfordshire. He has over 25 years of industry experience, starting in the field of telecommunications with Bell Northern Research and Nortel Networks, working on both SDH and wireless technologies. For the latter 18 years, he has been working for Spirent Communications within the GNSS/INS simulation industry. While working for Spirent, he has delivered diverse positioning solutions from hand-set to space vehicle applications, with a current focus on connected autonomous vehicles. He also works as a volunteer with The National Botanic Garden of Wales, developing software solutions for the Gardens' research programme that utilizes genomic approaches for biodiversity conservation. He is currently the Technical Innovation Engineer (Principle Engineer) with the Positioning Technology Business Unit, Spirent Communications plc.

MATTHEW D. HIGGINS (Senior Member, IEEE) received the M.Eng. degree in electronic and communications engineering and the Ph.D. degree in engineering from the School of Engineering, University of Warwick, in 2005 and 2009, respectively. He then progressed through several Research Fellow positions, in association with some of the U.K.'s leading defense and telecommunications companies before undertaking two years as a Senior Teaching Fellow in telecommunications, electrical engineering, and computer science subjects. In July 2012, he was promoted to Assistant Professor, where his research focused on optical, nano, and molecular communications, while in this position, he set up the Vehicular Communications Research Laboratory which aimed to enhance the use of communications systems within the vehicular space. In March 2016, he was promoted and appointed as an Associate Professor with WMG working in the area of connected and autonomous vehicles, where he leads the ICT and 5G themes of the group. He is also a FHEA and a member of the EPSRC CommNet2 and the EPSRC Peer Review College.