CARMEN: Center for Automated Vehicle Research with Multimodal Assurred Navigation

A USDOT Tier-1 University Transportation Center

Literature Review of PNT and GNSS Threats and Vulnerabilities to HATS

Qadeer Ahmed (https://orcid.org/0000-0002-4438-8663)

FINAL RESEARCH REPORT - October 20, 2022

Contract # 69A3552047138

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated in the interest of information exchange. This report is funded, partially or entirely, by a grant from the U.S. Department of Transportation's University Transportation Centers Program. The U.S. Government assumes no liability for the contents or use thereof.

1 Acronyms

ADC	analog-to-digital converter
ADAS	automated driver assistance systems
ADS	Automated Driving System
ADS-B	Automatic Dependent Surveillance-Broadcast
AGV	automated ground vehicle
AIM	Autonomous Intersection Management
AIS	Automatic Identification System
AOA	angle-of-arrival
A-PNT	assured PNT
ASIC	application-specific integrated circuit
ASIL	Automotive Safety Integrity Level
AWGN	additive white Gaussian noise
CACC	Cooperative Adaptive Cruise Control
CDGNSS	carrier-phase differential GNSS
CNN	Convolutional Neural Network
CRLB	Cramer-Rao Lower Bound
CST	Compound Scalar Testing
CUSUM	Cumulative Sum
DTG	Dynamically Tuned Gyroscopes
DoS	Denial of Service
DLN	deep-layered navigation
DSRC	Dedicated short-range communication
ECDSA	elliptic curve digital signature algorithm
EKF	Extended Kalman Filter
Faster-RCNN	Faster Region-based Convolutional Neural Network
FDOA	frequency difference of arrival
FDI	False Data Injection
FMCW	Frequency-modulated-continuous-wave
FMEA	Failure Modes and Effects Analysis
FOG	Fiber-Optic gyroscopes
FOTON	Fast, Orbital, TEC, Observables, and Navigation
FPGA	Field-Programmable Gate Array
FTA	Fault Tree Analysis
GIS	Geographic Information System
GLR	Generalized Likelihood Ratio
GNSS	Global Navigation Satellite System
GPP	general-purpose processor
GPS	Global Positioning System
HATS	Highly Automated Transportation System
HD	High-Definition
HAVs	Highly Automated Vehicles
HAZOP	Hazard and Operability Study

HITL	Human in the Loop
HTTPS	Hypertext Transfer Protocol Secure
IF	intermediate frequency
IGS	International GNSS Service
ILS	integer least squares
IMU	Inertial Measurement Unit
INS	Inertial Navigation System
IRTAD	International Traffic Safety Data and Analysis Group
ISO	International Organization for Standardization
ISS	International Space Station
KF	Kalman Filter
LEO	low Earth orbit
LiDAR	Light Detection and Ranging
LSTM	Long Short Term Memory
LTE	long term evolution
MAC	message authentication code
MAVs	Micro aerial vehicles
MBS	Metropolitan Beacon System
MEMS	Micro-Electro-Mechanical Systems
MEO	medium Earth orbit
MIMO	multi-input multi-output
MINOLESS	Minimum Norm Least Squares Solution
ML	Machine Learning
MOT	Minimum Operational Threshold
MSCKF	multi state constraint Kalman filter
MSF	Multi Sensor Fusion
NDT	Normal Distributions Transform
NLOS	Non-Line of Sight
NMA	navigation message authentication
NME	navigation message encryption
NHCs	non-holonomic constraints
ODD	Operational Design Domain
OFDM	Orthogonal frequency-division multiplexing
OBU	On-Board Unit
OSNMA	Open Service Navigation Message Authentication
PNT	Positioning, Navigation and Timing
P2PCD	Peer-to-Peer Certificate Distribution
POD	precision orbit determination
PPP	precise point positioning
PVT	Positioning, Velocity and Timing
QCD	quickest change detection
RF	Radio Frequency
RFI	radio-frequency interference
RLG	Ring Laser Gyroscopes
RL	Reinforcement Learning

RNL	Radio navigation Lab
RSS	received-signal-strength
RSU	Roadside Unit
RTK	Real-Time Kinematic
SAW	surface acoustic wave
SCA	spreading code authentication
SCE	spreading code encryption
SCER	security code estimation and replay
SDR	software-defined radio
SIS	signal-in-space
SIMD	single instruction, multiple data
SLAM	simultaneous localization and mapping
SNR	signal-to-noise ratio
SOPs	Signals of Opportunity
SOTIF	Safety of the Intended Funcionality
SPRT	Sequential Probability Ratio Test
SQM	signal-quality-monitoring
SSA	spectrum situational awareness
SSO	Sun-synchronous orbit
STL	Smart Traffic Light
STPA	System Theoretic Process Analysis
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege
SVs	space vehicles
SVM	Support Vector Machine
TCD	transient change detection
TDOA	Time-difference of arrival
TESLA	timed efficient stream loss-tolerant authentication
TLS	Transport Layer Security
TOA	time-of-arrival
TTC	Time To Collision
TTFAF	time-to-first-authenticated-fix
TRNS	terrestrial radio navigation systems
UAM	urban air mobility
UAV	Unmanned Aerial Vehicle
UE	user-equipment
UKF	Unscented Kalman Filter
UWB	ultra wideband
V2I	Vehicle to Infrastructure
V2P	Vehicle to Pedestrian
V2V	Vehicle to Vehicle
VANET	Vehicular Ad-hoc Network
V2X	Vehicle to Everything
VDCs	vehicle dynamics constraints
VRUs	Vulnerable Road Users

WLAN	Wireless Local Area Network
YOLO	You Only Look Once
ZUPT	zero velocity update

Abstract

We conducted a thorough literature survey on topics relevant to assured PNT for automated vehicles. The presented literature gathers and systematizes existing knowledge related to the system components of PNT and HAV systems. In particular, it treats opportunities, threats, and vulnerabilities related to (1) inertially-coupled GNSS receivers, (2) non-GNSS radio navigation via signals of opportunity (SOPs) and dedicated terrestrial beacons, (3) radar, lidar, and vision systems, (4) communications between vehicles and data/computation stored in cloud and edge servers, and (5) cooperative sensing: communication between vehicles and other traffic participants and infrastructure. This literature review also focuses on analyzing, (6) multi-sensor fusion strategies, attacks, detection, and mitigation mechanisms as found in the literature focusing on ground and aerial vehicles.

We have summarized a series of prior survey articles and book chapters that we have identified as the state of the art in recent years, including the definitive book chapter on GNSS interference written by Humphreys, and the definitive book chapter on GNSS spoofing and detection co-authored by Humphreys. We categorized and systematized the evaluation of top strategies for GNSS authentication and GNSS resilience by extending the approach that Humphreys. We have extended this work to include GNSS spoofing defenses and attacks introduced since 2016, such as the flexible multi-antenna meaconing attack and NovAtel's layered defense, as well as GNSS denial of service (jamming). We have identified the schemes for GNSS signal authentication and resilience that are well suited to implementation on highly automated vehicles (HAVs), such as those that exploit inertial sensing, multiple antennas, and signal quality monitoring.

We have identified terrestrial and LEO satellite signals of opportunity (SOPs) that could provide PNT for ground and aerial HAVs, with a focus on SOP-derived PNT integrity, availability, accuracy, and security. We have studied PNT security, continuity, and resiliency of dedicated terrestrial beacons (e.g., NextNav), which could be well suited to play a role as a GNSS backup for future HAVs.

HAVs, whether ground, aerial, or maritime, depend crucially on RADAR, LiDAR, and vision systems for collision avoidance and PNT. The use and performance of these technologies have been extensively covered in the literature, but their PNT impacts have seen little scrutiny. We have reviewed the RADAR, LiDAR, and vision literature, points out gaps in current knowledge, and develops studies within the CARMEN UTC to address these gaps.

High-definition (HD) maps stored in cloud or edge servers are a key asset for HATS: they enable vehicles to "expect the expected" in route planning and perception. These maps are essential for PNT because local sensing data are compared against them for localization. We have assessed the vulnerability of vehicles to disruption or manipulation of vehicle-to-cloud/edge communication.

Cooperative sensing is a paradigm in which multiple vehicles and infrastructure exchange sensor data in real time to amplify each vehicle's situational awareness. Low-rate V2X protocols, such as DSRC, are capable of exchanging fully-digested situational estimates,

such as vehicle poses, velocities, and hazard alerts. But to enable fuller situational awareness, a broader data-sharing regime is necessary, one that exchanges raw sensor data such as images, radar and lidar returns, and GNSS observables. We have assessed cooperative sensing opportunities and risks, including cooperatively derived PNT. An example of sensing opportunities and risks is shown in Figure 12

Multi-sensor fusion is the process of combining information from multiple sensors to produce a more accurate and comprehensive understanding of a situation or environment. In the context of security and defense, this can be used to improve the accuracy of surveillance and detection systems, for example by combining data from GNSS, INS, radar, cameras, and other sensors to track and identify potential threats.

Stealthy methods for attacking multi-sensor fusion systems involve techniques that aim to evade or deceive these systems without being detected. By disrupting or manipulating the data from one or more of these sources, an attacker could potentially create confusion or uncertainty in the fused data, making it more difficult for the system to accurately track or identify potential threats. As such, it is important for designers and operators of multi-sensor fusion systems to be aware of these potential attack vectors and take steps to both detect and mitigate these threats.

Our work has included USDOT guidance on PNT and existing information on GNSS vulnerabilities and integrity from publicly-available work from DoD, particularly as it relates to antenna systems and anti-jam techniques. Besides summarizing the state-of-the-art in these various categories, our review also identified the gaps in the current knowledge and practice.

Contents

1 Acronyms **i**

2 Vulnerabilities, Threats, and Mitigation Directly Affecting GNSS Devices **4**

2.1 GNSS Hardening 5

2.1.1 GNSS Receiver Development: 10

2.1.2 Natural Interference Mitigation: 13

2.1.3 Jamming and Spoofing Defenses: 19

2.2 Augmented PNT 21

2.2.1 Vision: 23

2.2.2 Radar 26

2.2.3 Lidar 28

2.2.4 Terrestrial Navigation Systems 29

2.2.5 Communication Systems 37

2.2.6 LEO PNT 40

2.3 Spectrum Situational Awareness 46

2.3.1 Interference Monitoring from LEO 47

2.3.2 Radar Interference 53

3 Vulnerabilities, Threats, and Mitigation for Local or Relative PNT Sensors **55**

3.1 Roadside Sensing Technologies 55

3.1.1 Pedestrian Safety 55

3.1.2 Classical Detection Technologies 57

3.1.3 Emerging Sensing Technologies 58

3.2 Threats and Vulnerabilities in Vehicle-To-Everything (V2X) Communication Protocols and Applications 69

3.3 Threats and Vulnerabilities in PNT Systems, Sensors and Sources for HAT 69

3.3.1 Waypoint Positioning System 71

3.3.2 Attitude determination system 72

3.3.3 Path-Planning System 72

3.3.4 Collision Avoidance System 73

3.3.5 Lane Keeping and Departure System 75

3.3.6 Adaptive Front Lighting System 76

3.3.7 Traffic Sign Recognition System 77

3.3.8 Night Vision System 77

3.3.9 Emergency Braking System 77

3.3.10 Pedestrian Detection System 79

3.3.11 Blind Spot Detection System 80

3.3.12 Parking Assist System 81

3.3.13 Parking Space Detection System 83

3.3.14 Valet Parking System 85

3.3.15 Auto Summon System 86

3.3.16 Adaptive Cruise Control System 86

4 Vulnerabilities, Threats, and Mitigation for PNT Information in HAT Systems 91

4.1 Roadside Sensing Technologies 92

4.2 Sensor Fusion 92

4.3 Crowdsourcing 93

4.4 Vehicle to Pedestrian (V2P) 94

5 Survey on Multisensor Fusion Localization: methods, attacks, detection and mitigation strategies 98

5.1 Introduction 98

5.2 Multisensor fusion for localization 98

5.2.1 Background 99

5.3 Taxonomy 100
5.4 MSF estimation methods for localization 102
5.5 Cyber-physical attacks overview 103
5.5.1 Classification based on Stealthiness 104
5.5.2 Classification based on Attack objective 106
5.6 Attack detection 107
5.7 Mitigation strategies 108
5.8 Risk assessment strategies 109
5.9 Discussion 112

2 Vulnerabilities, Threats, and Mitigation Directly Affecting GNSS Devices

Highly automated transportation systems rely on a steady stream of signals and information from external sources for localization, route planning, perception, and general situational awareness. This includes reliance on positioning, navigation, and timing (PNT) information: Location is essential for autonomous navigation and planning; and accurate timing is a precondition for on-board sensor fusion, cooperative control, and management based on information from other vehicles or the infrastructure. It is crucial to identify schemes for GNSS signal authentication and resilience that are well-suited for highly autonomous vehicles (HAVs). HAVs require PVT sensing techniques that are resilient to unusual natural or accidental events and secure against deliberate attack.

GNSS will no doubt play a significant role in PNT for HAVs, as GNSS is the only positioning system that offers absolutely-referenced meter-level accuracy with global coverage and all-weather operation. Furthermore, carrier-phase differential GNSS (CDGNSS), whose real-time variant for mobile platforms is commonly known as real-time kinematic (RTK) GNSS, is a centimeter-accurate positioning technique that differences a receiver's GNSS observable with those from a nearby fixed reference station to eliminate most sources of measurement error. The trouble is that GNSS is fragile: the harsh multi-path and signal blockage conditions of the urban ground vehicle environment often result in degraded position estimation. Furthermore, GNSS is susceptible to deliberate attack, as its service is easily denied by jammers, or deceived by spoofers. Fig. 1 provides an overview of different types of radio frequency (RF) interference the GNSS receiver on an HAV may encounter.

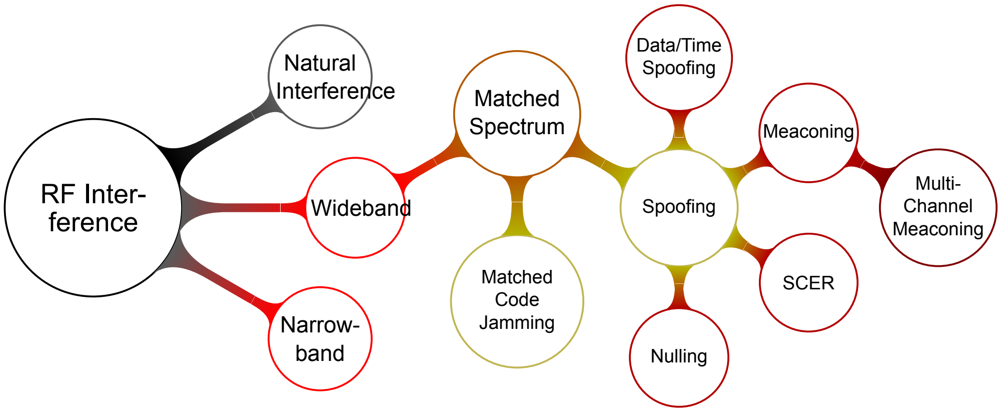


Figure 1: A taxonomy of RF interference threats to GNSS receivers.

Fortunately, significant advancements in PNT resiliency have been made over the past two decades. Fig. 2 shows a taxonomy of defenses against GNSS interference that HAVs may wish to employ. The first type of defense is GNSS hardening. The idea of GNSS hardening is to toughen the GNSS receiver against interference specific to GNSS. At the core of

GNSS-hardened systems is inertial navigation, which is a ubiquitous pairing alongside GNSS receivers. Inertial Measurement Units (IMU) are impervious to RF interference and signal blockage. Tightly coupling GNSS receivers with IMUs enable precise navigation in challenging multi-path environments and provide a powerful defense against spoofing.

The next strategy for PNT resiliency is augmenting GNSS. Traditional GNSS has been brilliantly successful, yet for some applications, they remain inadequate with regard to the accuracy, constellation survivability, or robustness to interference—for both civil and military users. To address these limitations, several alternative augmentation systems have been investigated such as: (1) Vision-based; (2) Radar-based; (3) terrestrial radio navigation systems (TRNS); (4) Communication systems; (5) LEO PNT; and (6) Signals of Opportunity. These alternate sensors can be either coupled with GNSS or operate as stand-alone PNT solutions in GNSS-denied environments.

Finally, the last form of PNT resiliency is spectrum situational awareness (SSA). Interference can present itself anywhere across the RF spectrum as attackers can target any subsystem of sensors on the HAV (e.g. GNSS receiver and FMCW radar). Identifying when and where a receiver is affected by interference is an important first step toward locating and mitigating the interference itself.

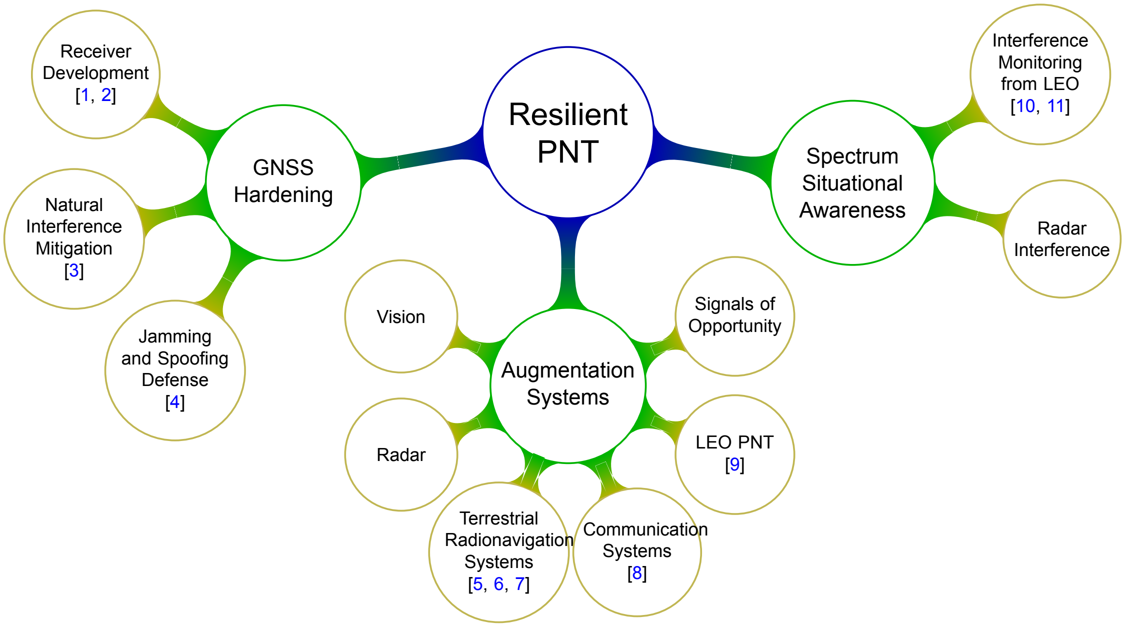

Resilient PNT
GNSS Hardening
Receiver Development [1, 2]
Natural Interference Mitigation [3]
Jamming and Spoofing Defense [4]
Augmentation Systems
Vision
Radar
Terrestrial Radionavigation Systems [5, 6, 7]
Communication Systems [8]
LEO PNT [9]
Signals of Opportunity
Spectrum Situational Awareness
Interference Monitoring from LEO [10, 11]
Radar Interference

Figure 2: A taxonomy of defenses against RF interference. The cited papers were developed under CARMEN.

2.1 GNSS Hardening

A typical IMU comprises triad accelerometers and a triad of gyroscopes to capture the three-dimensional motion of the platform to which it is mounted. The accelerometers are

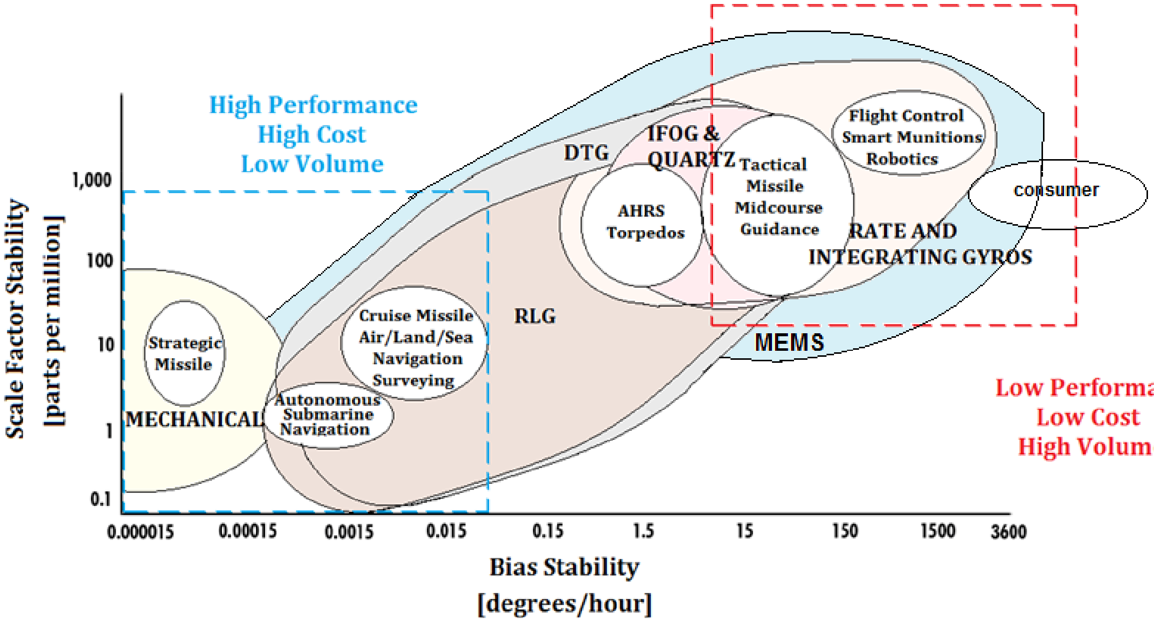


Figure 3: Relationship between scale factor stability and bias stability of different gyroscopes [12].

used to sense the specific forces or accelerations, while the gyroscopes are used to measure the angular rate of the platform's rotations, which are used to transform the sensed accelerations into a navigation frame. In principle, navigation based on IMU measurements only will be attained by integrating the accelerations over time with the knowledge of the initial positions and velocities of the platform.

Technologies for IMU sensors have evolved from pure mechanic-based technology to more advanced ones. Nowadays, accelerometers are typically based on mechanical pendulous, vibratory fiber optic, vibrating quartz, surface acoustic wave (SAW), and silicon. Similarly, current gyroscopes include mechanical gyroscopes, Ring Laser Gyroscopes (RLG), Fiber-Optic gyroscopes (FOG), Quartz, Dynamically Tuned Gyroscopes (DTG), Rate and Integrating Gyroscopes and Micro-Electro-Mechanical Systems (MEMS) [12, 13].

As with other measurement devices, IMU sensors also have some systematic and random errors. Systematic errors of the inertial sensors include bias, scale factor, scale factor non-linearity, and cross-coupling. A bias is a constant shift in the measured quantity from the actual input to the sensor. Whereas, a scale factor is an error that represents the mismatch between the input quantity and the reported output quantity of the sensor. Scale factor non-linearity refers to the effects of some environmental impacts and sensor designs that cause the scale factor to be no longer linear. Cross-coupling is caused by the non-orthogonality of the sensitive axes of inertial sensors. Random errors are acting as noises in the measurements [14, 13].

An illustration of the relationship between bias stability and scale factor stability of different gyroscopes in different application scenarios is shown in Figure 3 [12].

There is no universally agreed definition for categorizing inertial sensors [15]. Meanwhile, IMU sensors are roughly categorized into different grades per their performance, accuracy, and application scenarios. [16] categorizes IMU sensors into strategic, navigation, and tactical grades as in table 1. In [12], the tactical grade is classified further into high-end and low-end, and a consumer-grade is added as in table 2. A commercial grade, also called an automotive grade, is added in [13] as in table 2. From these tables, it can be found that some overlaps and mismatches exist in different categorizations.

Table 1: Specifications of the IMU sensors for different grades [16]

	Gyroscope		**Accelerometer**	
Grade	Bias [°/h]	SF [ppm]	Bias [μg]	SF [ppm]
Strategic	<0.0001	<50	<1	<2
Navigation	0.0001-0.1	1-100	1-1000	1-100
Tactical	0.1-10000	>100	50-10000	>100

SF: Scale factor

Table 2: Bias stability of different grades of gyroscopes [12]

Grade	**Bias [°/h]**	**Technology**	**Application**
Strategic	0.0001–0.01	RLG/FOG	Submarine navigation
Navigation	0.01-0.1	RLG/FOG	Aeronautics navigation
High-end Tactical	0.1–1	RLG/FOG	Missile navigation
Tactical	0.1–30	FOG/RLG	Platform stabilization
Industrial & Low-end tactical	1–30	MEMS	Ammunition & rocket guidance
Consumer	30-1000	MEMS	Motion interface

The integration of GNSS and IMU can be implemented in loosely coupled, tightly coupled, and deeply coupled modes. In loosely coupled mode, GNSS and inertial sensors individually process their raw measurements to obtain the navigation solution for each system; the final navigation solution and the inertial sensor errors are determined by fusing the two individual navigation solutions together. In tightly coupled mode, the GNSS and inertial sensors process their raw measurements simultaneously and optimally to estimate the position, velocity, and orientation of the platform together with the inertial sensor errors in a single filter. In deeply coupled mode, the integrated navigation solution is fed back to predict the code and carrier-phase pseudo-ranges of the GNSS receiver to aid the carrier tracking loops in the high-dynamic or jamming environments [17].

Hardening GNSS receivers against natural and deliberate interference is paramount for the safe and reliable operation of HAVs. The core of GNSS-hardened systems is inertial navigation, which is virtually impervious to radio frequency (RF) interference, poor weather, signal blockage, and data ambiguity. Inertial sensors are central to low-cost ground-vehicle robustness against natural and deliberate interference. Incorporating measurements from an inertial measurement unit (IMU) is a natural solution to bridge availability gaps in urban CDGNSS due to the adverse signal environment.

Furthermore, inertial systems provide the basis for sensitive GNSS spoofing detection. IMU-based GNSS spoofing detection capitalizes on a simple but consequential observation: it is practically impossible for a spoofer to create a false ensemble of GNSS signals whose carrier phase variations when received through the antenna of a target ground vehicle, track the phase values predicted by inertial sensing. In other words, antenna motion caused by road irregularities, or rapid braking, steering, etc., is sensed with high fidelity by an onboard IMU but is unpredictable at the sub-cm level by a would-be spoofer. Therefore, the differences between IMU-predicted and measured carrier phase values offer the basis for an exquisitely sensitive GNSS spoofing detection statistic.

The UT Radio Navigation Lab (RNL) has made strides in Software-Defined Radio (SDR) developments for GNSS. [1] proposes a framework for structuring data bit transfers from the radio frequency (RF) front-end to a General-Purpose Processor (GPP) in SDR for Global Navigation Satellite System (GNSS) applications. With the evolution of multi-antenna and multi-frequency GNSS SDRs, the packing and unpacking of data bits between the RF front-ends and GPP becomes increasingly complicated. ION's Metadata Standard provides a foundation for standardizing GNSS SDR output files but does not accommodate data packing formats that are efficient for processing by an important class of SDRs are called bit-wise SDRs. Besides proposing an extension to the ION Metadata Standards that resolve this shortcoming, this paper treats the problem of bit-packing for bit-wise SDRs more generally: It develops a bit-packing scheme that is flexible enough to accommodate any practical combination of antennas, frequency bands, sampling rates, and quantization encodings while optimizing bit-wise SDR processing efficiency within the constraints of low-cost front-end hardware. The performance of the proposed scheme is presented in terms of reduced instructions per processed sample. Performance is validated experimentally by implementing the proposed scheme on a high-performance GNSS SDR whose dual-antenna, tri-band RF front-end was recently developed in house at the University of Texas Radio Navigation Laboratory.

[2] explores how advancements in computer processing, both in a single instruction, multiple data (SIMD), and multi-core technology, have shaped the growth of software-defined Global Navigation Satellite Systems (GNSS) receivers. Historically, GNSS software-defined radio (SDR) has been limited to research and development purposes. But now, modern processor architectures and instruction sets are particularly efficient, paving the way for more capable SDR. GRID, the GNSS SDR developed in the Radio navigation Lab, has recently achieved a remarkable inflection point: under some processing configurations, the correlation operation, by which each channel's signal is mixed to baseband and de-spread via multiplication against a local code replica, is no longer the bottleneck process. This important milestone in pure software-defined GNSS makes SDR is a formidable competitor against traditional mass-market application-specific integrated circuit (ASIC)-based GNSS receivers. Further, this paper offers an exploration of commercial use cases particularly well-suited for GNSS SDR: space applications, wall-mounted electronic technologies, and automated vehicles. In detailing the status of GRID and its various applications, this pa-

per presents the case that software-defined GNSS is ready for launch for mass market applications, rather than solely a tool for research and development.

Advancements in precise positioning in deep urban environments were made in [3]. A vehicular pose estimation technique is presented that tightly couples multi-antenna carrier-phase differential GNSS (CDGNSS) with a low-cost MEMS inertial sensor and vehicle dynamics constraints. This work is the first to explore the use of consumer-grade inertial sensors for tightly-coupled urban CDGNSS, and first to explore the tightly-coupled combination of multi-antenna CDGNSS and inertial sensing (of any quality) for urban navigation. An unscented linearization permits ambiguity resolution using traditional integer least squares while both implicitly enforcing known-baseline-length constraints and exploiting the multi-baseline problem's inter-baseline correlations. A novel false fix detection and recovery technique is developed to mitigate the effect of conditioning the filter state on incorrect integers. When evaluated on the publicly-available TEX-CUP urban positioning data set, the proposed technique achieves, with the consumer- and industrial-grade inertial sensors, respectively, a 96.6% and 97.5% integer fix availability, and 12.0 cm and 10.1 cm overall (fix and float) 95th percentile horizontal positioning error.

GNSS security was enhanced in [4], where the authors developed, implemented, and validated a powerful single-antenna carrier-phase-based test to detect GNSS spoofing attacks on ground vehicles equipped with a low-cost IMU. This spoofing detection technique capitalized on the carrier phase fixed-ambiguity residual cost produced by a well-calibrated carrier-phase-differential GNSS (CDGNSS) solution that is tightly coupled with a low-cost IMU. The finer movements of the vehicle, such as slight steering movements and road vibrations, are the necessary unpredictable dithering a spoofer is not able to replicate. The differences between IMU-predicted and measured carrier phase values offer the basis for an exquisitely sensitive GNSS spoofing detection statistic. It is demonstrated that high-sensitivity spoofing detection is possible despite integer folding and urban multi-path. Artificial challenging spoofing attacks were injected into a data set collected by a vehicle-mounted sensor suite and detected within two seconds. This level of sensitivity to spoofing with only a single antenna and low-cost IMU is unprecedented. The type of tightly-coupled IMU-GNSS estimator whose by-products the proposed detection technique exploits is not currently available on commercial passenger vehicles but can be expected to be adopted in future automated vehicles since it provides all-weather dm-level absolute positioning at a minimal financial burden.

The following section outlines schemes for GNSS hardening and signal authentication that are well suited to implementation on HAVs. The GNSS hardening techniques are presented in the following order: (1) GNSS Receiver Development; (2) Natural Interference Mitigation; and (3) GNSS Jamming and Spoofing Defenses.

2.1.1 GNSS Receiver Development:

Software-defined GNSS, in which all GNSS receiver signal processing downstream of sampling and quantization is performed on a general-purpose processor rather than an ASIC or FPGA, has seen its fortunes rise, fall, and rise again over the past quarter century. In 1996, GPS pioneer Philip Ward pronounced software-defined GNSS dead on arrival: “It is unlikely that the speed-power product of general purpose digital signal processors will make them the suitable choice to perform the code and carrier wipe-off function in the near future, perhaps never” [18]. The only GNSS SDR at the time was Dennis Akos’s GPS/GLONASS SDR, which featured a novel front-end design that permitted sampled data collection and storage, but did not have the computational power to continuously track GNSS signals in real-time [18]. In 1999, the first GNSS SDR that operated in “real-time” operation emerged from Akos and co-authors in [19], which was able to process 60 seconds of IF data in 55 seconds. This effort was a notable achievement in the history of the GNSS SDR. In 2004, Brent Ledvina and co-authors presented the first real-time dual-frequency (L1 C/A, L2C) software-defined GPS receiver, which supported 10 tracking channels [20]. 2007 was a banner year for GNSS SDR: Cambridge Silicon Radio spent $75M to buy NordNav, a Swedish company that had developed a software-defined GNSS receiver for use in cell phones and other embedded applications. CSR’s purchase sparked great commercial interest in SDR technology. But the marginal power draw increase due to the NordNav SDR solution, although remarkably low for an SDR, was still too high for mass market cell phones. On this realization, CSR mothballed the NordNav software, opting instead to buy SiRF, which offered a high-performance, low-power, ASIC-based solution.

By 2016, embedded processing power had become more efficient. In that year, Trimble rolled out a software-defined GNSS receiver called Catalyst for widespread commercial use. The Trimble Catalyst SDR consumed digitized data from a radio frequency (RF) front-end which was embedded in a handheld antenna (DA1). The SDR harnessed the processing power of a smartphone or tablet to compute a user’s position and time. DA2, Trimble’s second-generation Catalyst product, now bundles a processor with the antenna to relieve the burden on the phone, but the solution remains software-defined and thus maintains the attractive flexibility of GNSS SDR [21].

Now in 2022, advancements in processor speeds and parallel instructions and architectures have unlocked expanded possibilities. The following sections detail the current status and performance of a state-of-the-art software-defined GNSS receiver, GRID. The GRID receiver exploits parallelism at multiple levels of operation: (1) it performs correlation using the bit-wise parallel technique developed by Psiaki and Ledvina [22], (2) it supports hundreds of channels in real-time by distributing processing across multiple general purpose cores [23], and (3) it makes full use of single-instruction multiple-data (SIMD) instructions to accelerate correlation arithmetic and bit manipulation.

Harnessing the latest SIMD instruction sets, GRID’s performance has recently achieved a remarkable inflection point: under some processing configurations, the correlation operation is no longer the bottleneck process. This represents a major milestone for software-defined GNSS: the very operation that Philip Ward warned in 1996 that could make general-purpose processors perpetually unsuitable for GNSS signal processing is now so efficiently implemented that it requires less then half the computational resources. GRID has become more capable and power-lean GNSS SDR by leveraging these technological advancements.

GNSS SDR from its inception has been a valuable platform and tool for research and development (R&D). Efficient, low-power, low-cost multi-core processors developed for smartphones, together with new algorithms tailored to exploit parallelism, have now made GNSS SDRs ready for widespread commercial use, not just for R&D. Some commercial uses for which GNSS SDR is particularly well-suited for our space- and aerial applications, wall-mounted electronic technologies, automated vehicles, and a host of emerging technologies that require a high-performance GNSS solution.

[2] provides a comprehensive description of the state-of-the-art in pure GNSS SDR based on bit-wise parallel correlation, an explanation of how modern processor architectures and instruction sets have led to an inflection point in which correlation is no longer the processing bottleneck, and an exploration of use cases particularly well suited for GNSS SDR.

Within the past decade, software-defined radios (SDRs) have emerged as an especially valuable platform for GNSS research and development [24]. GNSS-SDRs implementations vary greatly but are characterized by processing more-or-less-raw samples of radio frequency (RF) data from an analog front-end using general-purpose processors, either online (i.e. in real-time) or offline (i.e. post-processing). Because they enable researchers to collect and share large raw-sample data sets, GNSS SDRs are an ideal tool for collaboration and repeatable, high-fidelity cross-verification within the GNSS community.

The lack of a standardized data format for raw RF data previously stymied this process. Properly importing a data set into a software package different from that used for the original recording could be error-prone and tedious. To tackle this problem, the Institute of Navigation (ION) GNSS SDR Standard Working Group recently released their GNSS SDR Metadata Standard [25]. The Standard defines the structure of a machine- and human-readable auxiliary file to be distributed alongside raw-sample data sets. The introduction of this “metadata” is a much-welcomed initiative that promises to eliminate formatting ambiguities and promote interoperability in GNSS-SDR research. Not all GNSS-SDR implementations have quite the same requirements for their data formats. GNSS SDRs with software correlators may be sub-divided into byte-wise and bit-wise categories. Byte-wise SDRs represent each real or imaginary component of a front-end sample as a byte (e.g., the MuSNAT and the IFEN SX3 [26, 27]). As the smallest directly-addressable unit of computer memory and the smallest supported integer data type on most modern architectures, bytes represent an inflection point in software complexity. Operations on narrower quantization are less straightforward to implement.

Why might narrower quantization be desirable? The weak nature of GNSS signals-in-space and the typical hemispherical pattern of GNSS receiver antennas mean that as much as 99% of the power in a recorded GNSS-SDR waveform is additive white Gaussian noise (AWGN). At such a low signal-to-noise ratio (SNR), the formal information content of the desired signal cannot exceed a small fraction of a bit per sample. The bulk of the data set is noise. Bit-wise SDRs exploit the uneven distribution of this fraction-of-a-bit of useful information among the output bits of the analog-to-digital converter (ADC). Under these conditions, there are diminishing returns to each bit of quantization after the first. Bit-wise SDRs, therefore, truncate samples, sometimes to a single bit, to reduce memory bandwidth and power consumption (e.g., the UT Austin GRID SDR [28, 29, 23, 30]).

Version 1.0 of the Standard does not support the data formats that are most efficient for bit-wise SDR processing: those in which parallel planes of bits (e.g. sign bits, magnitude bits) from a single stream of RF, samples are aggregated (grouped into runs) rather than collated (interleaved). This renders two recently-offered public GNSS data sets, the University of Texas Challenge for Urban Positioning (TEX-CUP) [31], and the ATX Urban Positioning Challenge Data set [30], incompatible with the Standard. [1] proposes extensions to the Standard to improve compatibility with bit-wise SDRs.

Why should such an unusual bit-ordering be valuable? Since modern processors do not offer native arithmetic on data types smaller than a byte, bit-wise SDRs rely instead on “bit-slicing”: a digital logic circuit (AND, OR, NOT, XOR) for correlation is designed and implemented as a program with one Boolean instruction per gate. Each wire in the logic circuit is represented by a register-sized integer (a “word”), and the n^{th} bit of one word interacts only with the n^{th} bits of other words: that is, parallel bits flow through separate, parallel copies of the logic circuit. The correlator, therefore operates on as many samples in parallel as there are bits in a word. It is this mapping of logical wires to register-sized integers that leads to the bit-ordering preferences of bit-wise SDRs. Just as a 2×2-bit adder circuit uses distinct wires for high and low bits, the bit-sliced implementation uses different registers and memory locations to hold (corresponding vectors of) high and low bits. What would be a single instruction (multiply and add bytes) in a byte-wise SDR becomes many instructions; but data parallelism is fully exploited, critical paths are short, and the processor can be kept busy with many inexpensive Boolean operations. Bit-slicing is simplest when the depth of quantization is just one or two bits, but the technique does not have a strict limit.

[1] lays out proposed extensions to the Standard in concrete detail for encoding *arbitrary* packing of raw GNSS data sampled from potentially multiple antennas, frequency bands, quantization schemes, and sample rates. Additionally, [1] presents a scheme for efficient packing and unpacking of GNSS data streams. This scheme automatically generates compact packing logic and fast unpacking code from a description of the packed data format. Experimental results on x86-64 and ARM64 architectures demonstrate the tools’ efficiency and flexibility.

Both bit-wise and byte-wise GNSS-SDR implementations exploit vectorized processor instructions, known as Single Instruction, Multiple Data (SIMD). SIMD instructions are ideal for calculations with high data parallelism, such as correlation, because they operate on multiple samples in the same cycle. Typical vector register sizes range from 128 to 512 bits, though the largest sizes are not available on all processors. Most x86-64 processors outside of data centers, for instance, support up to 256-bit vector operations, while modern 64-bit ARM processors typically support only 128-bit SIMD instructions.

Depending on the CPU's particular SIMD instruction set, byte-wise SDRs can multiply and accumulate 16 samples per cycle per core [23], and bit-wise SDRs can multiply and accumulate 128 samples per core using a short sequence of SIMD XOR, `popcount`, and table look-up operations [22, 32, 33, 23]. The required memory bandwidth is lesser for bit-wise SDRs than for byte-wise SDRs. On the other hand, byte-wise SDRs eliminate quantization losses and are more easily adapted for use with non-binary modulation schemes like CBOC. Moreover, under non-AWGN conditions, greater quantization depth may be beneficial for e.g. adaptive notch filtering [34].

While graphics processing units (GPUs) might appear to be a compelling alternative, with their support for a stupendous amount of data-parallel computation in integer or floating-point formats [35], they suffer from high overhead in GPU/CPU communication and are therefore of the greatest use in the search phase of signal acquisition rather than during tracking.

2.1.2 Natural Interference Mitigation:

Future Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) connectivity will permit vehicles to relay their positions and velocities to each other with millisecond latency, enabling tight coordinated platooning and efficient intersection management. More ambitiously, broadband V2V and V2I enabled by 5G wireless networks will permit vehicles to share unprocessed or lightly-processed sensor data. *Ad-hoc* networks of vehicles and infrastructure will then function as a single sensing organism. The risk of collisions, especially with pedestrians and cyclists—notoriously unpredictable and much harder to sense reliably than vehicles—will be significantly reduced as vehicles and infrastructure contribute to sensor data from multiple vantage points to build a blind-spot-free model of their surroundings.

Such collaborative sensing and traffic coordination require vehicles to know and share their own position. How accurately? The proposed Dedicated Short Range Communications (DSRC) basic safety message, a first step in V2V coordination, does not yet define a position accuracy requirement, effectively accepting whatever accuracy a standard GNSS receiver provides [36]. But automated intersection management [37], tight-formation platooning, and unified processing of sensor data—all involving vehicles of different makes that may not share a common map—will be greatly facilitated by globally-referenced positioning with sub-30-cm accuracy.

Poor weather also motivates high-accuracy absolute positioning. Every automated vehicle initiative of which the present authors are aware depends crucially on lidar or cameras for fine-grained positioning within their local environment. But these sensing modalities perform poorly in low-visibility conditions such as a snowy whiteout, dense fog, or heavy rain. Moreover, high-definition 3D maps created with lidar and camera data, maps that have proven crucial to recent progress in reliable vehicle automation, can be rendered dangerously obsolete by a single snowstorm, leaving vehicles that rely on such maps for positioning no option but to fall back on GNSS and radar to navigate a snow-covered roadway in low-visibility conditions. When, as is often the case on rural roads, such snowy surroundings offer few radar-reflective landmarks, radar too becomes useless. GNSS receivers operate well in all weather conditions, but only a highly accurate GNSS solution, e.g., one whose absolute errors remain under 30 cm 95% of the time, could prevent a vehicle's drifting onto a snow-covered road's soft shoulder. Code-and Doppler-based GNSS solutions can be asymptotically accurate (averaged over many sessions) to better than 50 cm, which may be adequate for digital mapping [38], but they will find it challenging to meet a 30 cm 95% stand-alone requirement, even with modernized GNSS offering wide-band signals at multiple frequencies.

Carrier-phase-based GNSS positioning—also referred to as precise GNSS positioning even though it actually offers absolute accuracy, not just precision (repeatability)—can meet the most demanding accuracy requirements envisioned for automated and connected vehicles, but has historically been either too expensive or too fragile, except in open areas with a clear view of the overhead satellites, for widespread adoption. Coupling a carrier-phase differential GNSS (CDGNSS) receiver with a tactical grade inertial sensor, as in [39, 40, 41, 42] enables robust high-accuracy positioning even during the extended signal outages common in dense urban areas. But GNSS-inertial systems with tactical-grade inertial measurement units (IMUs) cost tens of thousands of dollars and have proven stubbornly resistant to commoditization. Coupling a GNSS receiver with automotive- or industrial-grade IMUs are much more economical, and significantly improve performance, as shown in [43]. But such coupling only allows approximately 5 seconds of complete GNSS signal blockage before the IMU no longer offers a useful constraint for so-called integer ambiguity resolution [44], which underpins the fastest, most accurate, and most robust CDGNSS techniques, namely, single-baseline RTK, network RTK, and PPP-RTK [45, 46].

Previous research has suggested an inexpensive technique for robustifying RTK positioning: tightly coupling carrier-phase-based GNSS positioning with inertial sensing and vision [47, 48]. Such coupling takes advantage of the remarkable progress in high-resolution, low-cost cameras within the intensely competitive smartphone market. The current authors are engaged in developing a high-integrity RTK-vision system for high-accuracy vehicular positioning in rural and urban environments. Further coupling with radar will make the system robust to low-visibility conditions.

As a step toward this goal, it is of interest to evaluate the performance of stand-alone RTK techniques—those unaided by IMUs, odometry, or vision—in urban environments. Such a study will reveal why and when aiding is necessary, and how an RTK positioning system might behave if aiding were somehow impaired or unavailable, whether due to sensor faults or, in the case of exclusive visual aiding, poor visibility conditions.

Little prior work has explored unaided vehicular RTK performance in urban environments, no doubt because performance results have historically been dismal. Short-baseline RTK experiments between two vehicles in [49] revealed that multi-frequency (L1-L2) GPS and GLONASS RTK yielded poor results in residential and urban environments. Only along a mountain highway with a relatively clear view of the sky was the availability greater than 90% and accuracy better than 30 cm. RTK positioning in downtown Calgary was disastrous, with less than 60% solution availability and RMS errors exceeding 9 meters.

More recently, Li et al. [43] have shown that, with the benefit of greater signal availability, unaided professional-grade dual-frequency GPS + BDS + GLONASS RTK can achieve correct integer fixing rates of 76.7% on a 1-hour drive along an urban route in Wuhan, China. But Li et al. do not provide data on the incorrect fixing rate, nor a full error distribution, so the significance of their results is difficult to assess.

Recent urban RTK testing by Jackson et al. [50] indicates that no low-to-mid-range consumer RTK solution offers greater than 35% fixed (integer-resolved) solution availability in urban areas, despite a dense reference network and dual-frequency capability. A key failing of existing receivers appear to be their slow recovery after passing under bridges or overpasses.

[30] describes and evaluates an unaided RTK positioning system that has been designed for vehicular operation in both rural and urban environments. Preliminary performance results were published in a conference version of this paper [51]. The current paper improves on the conference version in four ways: (1) the test route is both more challenging and more comprehensive, (2) a proper independent ground truth trajectory is used as the basis of error evaluation, (3) data modulation wipe-off for improved carrier tracking robustness is applied not only on GPS L1 C/A signals, as previously, but now also on SBAS L1 signals, and (4) the performance benefit of vehicle GNSS antenna calibration is assessed.

[30] provides a demonstration of the performance that can be achieved with a low-cost software-defined unaided RTK GNSS platform in a dense urban environment, and an evaluation of the relative importance of various factors (e.g., data bit wipe-off, age of reference data, rover antenna calibration, reference network density) to the overall system performance. To stimulate further innovation in urban precise positioning, all data from [30]'s urban driving campaign has been posted at `http://radionavlab.ae.utexas.edu` under “Public Datasets,” including wide-band (10 MHz) intermediate frequency samples from both the reference and rover antennas, RINEX-formatted rover and reference observables, and the ground truth trajectory.

The rise of connected and automated vehicles has created a need for robust globally-referenced positioning with lane-level (e.g., sub-30-cm) accuracy [52]. Much automated ground vehicle (AGV) research focuses on the use of LIDAR and cameras for navigation, but these sensing modalities often perform poorly in low illumination conditions or during adverse weather such as heavy fog or snowy white-out. By contrast, positioning techniques based on radio waves, such as automotive radar or GNSS, are robust to poor weather and lighting conditions [53]. Recent work has found that fusing measurements from low-cost automotive radars with inertial sensing can provide lane-level accuracy in urban environments [53]. But radar-based positioning in a global coordinate frame requires the production and maintenance of radar maps, which is a time-consuming and costly endeavor.

GNSS signals provide a source of high-accuracy all-weather absolute positioning that does not require expensive investment in systems for map production, storage, maintenance, and dissemination. If the so-called integer ambiguities associated with the carrier phase measurements can be correctly resolved, carrier-phase-based GNSS positioning offers exquisite accuracy. However, GNSS signal blockage, diffraction, and multi-path effects make this family of techniques extremely challenging to use in urban areas. Carrier-phase differential GNSS (CDGNSS), whose real-time variant for mobile platforms is commonly known as real-time kinematic (RTK) GNSS is a centimeter-accurate positioning technique that differences a receiver's GNSS observables with those from a nearby fixed reference station to eliminate most sources of measurement error [54, Sec. 26.3]. Previous work by this paper's authors probed the limits of unaided CDGNSS in the deep urban environment, and found that the combination of a GNSS measurement engine optimized for urban positioning and robust estimation techniques for outlier exclusion make CDGNSS feasible in the deep urban environment [30]. But the unaided CDGNSS system described in [30] suffers from availability gaps of up to 90 seconds in duration, making it insufficient to serve as the sole navigation sensor for an AGV.

A natural method to bridge such availability gaps is to incorporate measurements from an inertial measurement unit (IMU). These measurements are uniquely valuable due to their invulnerability to environmental effects such as radio interference and weather. Combined GNSS and inertial navigation systems that incorporate only GNSS position solutions as measurements for a downstream navigation filter are termed *loosely coupled*, whereas *tightly coupled* systems directly incorporate raw GNSS observables (pseudorange, Doppler, or carrier phase) [54, Sec. 28.8]. While both loosely- and tightly-coupled aiding can bridge availability gaps, tightly coupled aiding additionally reduces these gaps' frequency and duration: the inertial sensor provides probabilistic constraints between GNSS measurement epochs that increase the success rate of carrier phase integer ambiguity resolution. These constraints additionally make the navigation solution observable with fewer GNSS measurements.

AGV navigation filter performance can be further improved by tight coupling with so-called vehicle dynamics constraints (VDCs). One such technique exploits the natural motion constraints of four-wheeled ground vehicles, commonly referred to as non-holonomic constraints (NHCs). A second VDC technique infers a lack of vehicle motion by monitoring, for example, wheel odometry ticks, or by detecting a lack of road vibration. This constraint is then enforced as a strong zero-velocity pseudo-measurement, called a zero velocity update (ZUPT) in the literature.

[3] extends the navigation filter component of the CDGNSS system described in [30] by tightly coupling with an inertial sensor and with vehicle dynamics constraints, and by incorporating measurements from multiple vehicle-mounted GNSS antennas. It also develops

a novel robust estimation technique to mitigate the effects of multi path and allow graceful recovery from incorrect integer fixes.

The performance of CDGNSS unaided by inertial sensing in urban environments has historically been poor. Experiments in [49] suffered from poor availability (<60%) and large positioning errors (>9m RMS) in suburban and urban environments. A 2018 assessment of commercial CDGNSS receivers found that no low-cost solution offered greater than 35% fixed-integer solution availability in urban environments [50]. [43] achieved a 76.7% unaided correct integer fixing rate in urban Wuhan, China using dual-frequency CDGNSS with a professional-grade receiver. In 2019, Humphreys et al. achieved an unaided correct integer fix rate of 84.8% in the urban core of Austin, Texas [30].

Tightly-coupled inertial aiding has long been employed as a method to increase CDGNSS solution availability and robustness. Early systems built around highly-accurate but expensive tactical-grade IMUs were capable of providing robust positioning in dense urban areas [39, 40, 41, 42]. The recent emergence of inexpensive consumer- and industrial-grade Micro-Electro-Mechanical systems (MEMS) inertial sensors has led to a new chapter of research in low-cost inertial aiding for urban CDGNSS.

[43] demonstrated that the tight coupling of single-antenna professional-grade GNSS measurements with an industrial-grade MEMS IMU increased the integer fix availability of single-frequency CDGNSS from 44.7% to 86.1% on a test route in urban Wuhan, China. However, the authors did not provide the GNSS dataset, information on the incorrect integer fix rate, or a full error distribution, making these results difficult to assess.

[3] is the first to demonstrate an increased CDGNSS integer fix rate in an urban environment via tight coupling with a *consumer-grade* inertial sensor. Furthermore, it incorporates vehicle dynamics constraints and multiple vehicular GNSS baselines. The system's performance is evaluated on a publicly-available urban positioning data set, allowing for a head-to-head comparison of techniques by the urban positioning research community.

One disadvantage of CDGNSS is that it requires observations from a nearby base station to eliminate modeling errors (e.g., for atmospheric delays or satellite clocks and orbits) common to both the base station (the reference) and the vehicle (the rover). Short-baseline CDGNSS, which offers the greatest robustness against urban multi path [55], is limited to reference-rover baseline lengths below approximately 10 km [56]. To avoid the requirement for a nearby base station, attention has recently focused on extending precise point positioning (PPP), which is based on precise orbit, clock, and atmospheric corrections, to urban areas by tight coupling with inertial sensors.

Rabbou et al. in 2015 explored the tight coupling of PPP with a tactical-grade inertial sensor in mostly open-sky conditions with simulated GNSS outages, achieving centimeter accuracy [57]. [58] and [59] extended tightly-coupled PPP to industrial-grade MEMS inertial sensors in highway and suburban environments. More recently, [60] demonstrated tightly-coupled PPP using both a geodetic-grade and a low-cost GNSS receiver and an industrial-grade MEMS sensor along an urban route in downtown Toronto, Canada, but only achieved meter-level accuracy when using the low-cost GNSS receiver. A draw-back of PPP-based positioning is that the aforementioned results all required a roughly 10-minute convergence period before producing an accurate navigation solution. Short-baseline CDGNSS positioning with a modern multi-frequency, multi-constellation receiver, by contrast, typically yields instantaneous initialization.

Recent research has also explored the tight coupling of CDGNSS measurements with vehicle dynamics constraints. [61] found in a simulation study using a realistic 3D map of an urban environment that a tightly-coupled CDGNSS system using GPS only could feasibly provide high-integrity decimeter-level positioning when aided with vehicle-dynamics constraints, a tactical-grade IMU, and odometry based on wheel-speed sensors. [62] tightly coupled single-antenna CDGNSS with non-holonomic constraints and a tactical-grade fiber-optic IMU, but only evaluated their system under open-sky GNSS conditions with simulated GNSS degradations.

The use of multiple GNSS antennas on the vehicle for CDGNSS offers four advantages. First, the full six-degree-of-freedom vehicle pose (position and orientation) becomes instantaneously observable when CDGNSS measurements are combined with the gravity vector as measured by an inertial sensor. With a single GNSS antenna, the vehicle yaw is observable only over multiple epochs, and only if the vehicle accelerates during the observations [63]. Second, the shared reference antenna creates redundancy in the measurement model that allows better ambiguity resolution performance than any CDGNSS baseline taken individually [64]. Third, the additional set of GNSS measurements at the second antenna provides reduced position estimation error. Fourth, a highly effective method for GNSS spoofing detection, the multi-antenna defense [65], can readily be implemented.

Multi-antenna GNSS has long been used for attitude-determination applications with snapshot estimation methods such as C-LAMBDA [66] and MC-LAMBDA [67], which provide globally-optimal single-epoch maximum-likelihood solutions to the full nonlinear GNSS attitude determination problem, and have been successfully extended to the pose estimation case [68]. Other work has incorporated special cases of *a priori* attitude information into the nonlinear solution process [69]. These snapshot methods, however, are computationally demanding, and their extension to recursive estimation for tight coupling with other sensors is not straightforward and remains unexplored.

[70] found that a hard constraint using an *a priori* known vehicle attitude to combine CDGNSS observations from multiple vehicle antennas can increase ambiguity resolution and urban CDGNSS performance. However, this method requires a highly-accurate independent source of attitude information, such as from an expensive gyrocompass-capable tactical-grade IMU following an initial static alignment period.

[64] proposed pose estimation based on multiple vehicle antennas for inland waterway navigation. This work sidestepped the complexity of C-LAMBDA or MC-LAMBDA by linearizing the attitude model in an extended Kalman filter (EKF) update and propagating the state with a simple motion model. This formulation was found to increase ambiguity resolution performance over either the positioning or attitude determination problems taken independently. However, the authors made no attempt to incorporate an inertial sensor

or additional motion constraints.

[71] developed a multi-antenna GNSS system for aircraft pose estimation that is tightly coupled with a MEMS inertial sensor, but only used CDGNSS for attitude measurements, relying on standard pseudo-range measurements for the estimator's position component.

[72] tightly coupled triple-antenna CDGNSS with an industrial-grade inertial sensor for a micro air vehicle navigation application, but only evaluated the system's performance over a single, short test flight in open-sky conditions, and did not compare against a "ground truth" reference.

Previous work [73, 74] by this paper's authors explored a sub-optimal "federated filtering" approach to the tightly-coupled multi-antenna CDGNSS + inertial problem, additionally incorporating monocular vision measurements in [73]. But the approach did not properly model the multi-antenna CDGNSS measurement update, instead of resolving the position and attitude baselines separately.

An estimation technique is presented in [3] that tightly couples multi-antenna CDGNSS with vehicle dynamics constraints and inertial measurements. It is the first in the open literature to explore the tightly-coupled combination of multi-antenna CDGNSS and inertial sensing for navigation in urban environments. Furthermore, it is the first to explore the use of *consumer-grade* inertial sensors for tightly-coupled deep urban CDGNSS. It also applies a novel application of the unscented transform for the multi-baseline CDGNSS integer ambiguity resolution and measurement update step, which widens the operating regime of the filter to allow significantly greater attitude uncertainty without suffering from the excessive integer least squares (ILS) failures seen by existing EKF approaches. A novel false fix detection and recovery technique is developed that limits the degree to which an incorrectly-resolved integer ambiguity can corrupt the tightly-coupled CDGNSS estimator's state.

It also provides a demonstration of state-of-the-art deep urban CDGNSS performance, achieving, by tight coupling with consumer-grade and industrial-grade inertial sensors, respectively, a 96.6% and 97.5% integer fix availability, and 12.0 cm and 10.1 cm overall (fix and float) 95th percentile horizontal positioning error on the publicly-available TEX-CUP urban positioning data set [31].

2.1.3 Jamming and Spoofing Defenses:

The combination of easily-accessible low-cost Global Navigation Satellite System (GNSS) spoofers and the emergence of increasingly-automated GNSS-reliant ground vehicles prompt a need for fast and reliable GNSS spoofing detection [75, 76]. To underscore this point, Regulus Cyber recently spoofed a Telsa Model 3 on autopilot mode, causing the vehicle to suddenly slow and unexpectedly veer off the main road [77]. Among GNSS signal authentication techniques, signal-quality-monitoring (SQM) and multi-antenna could be considered for implementation on ground vehicles [78]. However, SQM tends to perform poorly on dynamic platforms in urban areas where strong multipath and in-band noise are common [79, 80, 78, 81], and multi-antenna spoofing detection techniques, while effective [82, 65], are disfavored by automotive manufacturers seeking to reduce vehicle cost and aerodynamic drag. Thus, there is a need for a single-antenna GNSS spoofing detection technique that performs well on ground vehicles despite the adverse signal-propagation conditions in an urban environment.

In a concurrent trend, increasingly-automated ground vehicles demand ever-stricter lateral positioning to ensure the safety of operation. An influential recent study calls for lateral positioning better than 20 cm on freeways and better than 10 cm on local streets (both at 95%) [52]. Such stringent requirements can be met by referencing lidar and camera measurements to a local high-definition map [83, 84], but poor weather (heavy rain, dense fog, or snowy whiteout) can render this technique unavailable [53]. On the other hand, recent progress in precise (dm-level) GNSS-based ground vehicle positioning, which is impervious to poor weather, has demonstrated surprisingly high (above 97%) solution availability in urban areas [3]. This technique is based on carrier-phase differential GNSS (CDGNSS) positioning, which exploits GNSS carrier phase measurements having mm-level precision but integer-wavelength ambiguities [85].

Key to the promising results in [3] is the tight coupling of CDGNSS and IMU measurements, without which high-accuracy CDGNSS solution availability is significantly reduced due to pervasive signal blockage and multipath in urban areas (compare the improved performance of [3] relative to [30]). Tight coupling brings mm-precise GNSS carrier phase measurements into correspondence with high-sensitivity and high-frequency inertial sensing. The particular estimation architecture of [3] incorporates inertial sensing via model replacement, in which the estimator's propagation step relies on bias-compensated acceleration and angular rate measurements from the IMU instead of a vehicle dynamics model. As a consequence, at each measurement update, an *a priori* antenna position is available whose delta from the previous measurement update accounts for all vehicle motion sensed by the IMU, including small-amplitude high-frequency motion caused by road irregularities. Remarkably, when tracking authentic GNSS signals in a clean (open sky) environment, the GNSS carrier phase predicted by the *a priori* antenna position and the actual measured carrier phase agree to within millimeters.

[4] pursues a novel GNSS spoofing detection technique based on a simple but a consequential observation: it is practically impossible for a spoofer to create a false ensemble of GNSS signals whose carrier phase variations, when received through the antenna of a target ground vehicle, track the phase values predicted by inertial sensing. In other words, antenna motion is caused by road irregularities, or rapid braking, steering, etc., is sensed with high fidelity by an onboard IMU but is unpredictable at the sub-cm-level by a would-be spoofer. Therefore, the differences between IMU-predicted and measured carrier phase values offer the basis for an exquisitely sensitive GNSS spoofing detection statistic. What is more, such carrier phase fixed-ambiguity residual cost is generated as a by-product of tightly-coupled inertial-CDGNSS vehicle position estimation such as performed in [3].

Two difficulties complicate the use of fixed-ambiguity residual cost for spoofing detection.

First is the integer-ambiguous nature of the carrier phase measurement [85], which causes the post-integer-fix residual cost to equal not the difference between the measured and predicted carrier phase, as would be the case for a typical residual, but rather this difference modulo an integer number of carrier wavelengths. Such integer folding complicates the development of a the probability distribution for a detection test statistic based on carrier phase fixed-ambiguity residual cost.

The severe signal multipath conditions in urban areas create thick tails in any detection statistic based on carrier phase measurements. Setting a detection threshold high enough to avoid false spoofing alarms caused by mere multipath could render the detection test insensitive to dangerous forms of spoofing. Reducing false alarms by accurately modeling the effect of a particular urban multipath environment on the detection statistic would be a Sisyphean undertaking, requiring exceptionally accurate up-to-date 3D models of the urban landscape, including materials properties. [4] takes an empirical approach to these difficulties. It does not attempt to develop a theoretical model to delineate the effects of integer folding or multipath on its proposed carrier-phase fixed-ambiguity residual cost-based detection statistic. Rather, it develops null-hypothesis empirical distributions for the statistic in both shallow and deep urban areas and uses these distributions to demonstrate that high-sensitivity spoofing detection is possible despite integer folding and urban multipath.

2.2 Augmented PNT

The RNL has also explored several augmentations to GNSS for PNT. [6] aimed to augment terrestrial radio navigation systems (TRNS) with autonomous signal-situational-awareness capability, allowing TRNS operators to detect spoofing and meaconing attacks within their systems. Such a capability is necessary to address a vulnerability to certain replay attacks that remain even when TRNS signals are secured by navigation message encryption and authentication. Two signal authentication techniques are developed to detect a weak spoofing signal in the presence of static and dynamic multipath. Both are shown to be effective in simulations of the varied operating environments that TRNS will encounter. With autonomous signal situational awareness, TRNS gain a defensive capability that GNSS cannot easily match: a comprehensive defense against most man-in-the-middle attacks on position, navigation, and timing services.

The security of terrestrial radio-navigation systems (TRNS) has not yet been addressed in the literature. [7] builds on what is known about securing global navigation satellite systems (GNSS) to address this gap, re-evaluating proposals for GNSS security in light of the distinctive properties of TRNS. TRNS of the type envisioned in this paper are currently in their infancy, unburdened by considerations of backward compatibility: security for TRNS is a clean slate. [7] argues that waveform- or signal-level security measures are irrelevant for TRNS, preventing neither spoofing nor unauthorized use of the service. Thus, only security measures that modify navigation message bits merit consideration. This paper proposes orthogonal mechanisms for navigation message encryption (NME) and authentication (NMA), constructed from standard cryptography primitives and specialized to TRNS: message encryption allows providers to offer tiered access to navigation parameters on a bit-by-bit basis, and message authentication disperses the bits of a message authentication code across all data packets, posing an additional challenge to spoofers. The implementation of this proposal will render TRNS more secure and resilient than traditional civil GNSS.

[5] presents a method of tightly coupling carrier-phase-differential GNSS (CDGNSS) with terrestrial radio navigation system (TRNS) signals and data to build a robust positioning, velocity, and timing (PVT) solution for urban air mobility (UAM). UAM will require precise and robust PVT solutions that are resilient to interference and jamming. CDGNSS offers absolute positioning with high availability and sub-decimeter accuracy but cannot serve as the sole source of PVT for UAM because of its vulnerability to interference: a single potent GNSS jammer could deny UAM service across an entire city where GNSS the sole means UAM navigation. TRNS signals are stronger than those of GNSS and offer additional frequency diversity. Their multipath errors, although larger than for GNSS at street level due to the low elevation angles with which TRNS signals propagate from terrestrial transmitters, are manageably small at altitudes where UAM vehicles will operate. Thus, TRNS offers an attractive backup to GNSS for UAM. This paper explores two techniques for the fusion of TRNS and CDGNSS: loosely- and tightly-coupled. The loosely-coupled technique fuses information from the two sensing modalities at the level of full PVT solutions. The tightly-coupled technique explored here fuses GNSS carrier phase and pseudo-range measurements with TRNS pseudo-range, Doppler, and calibrated pressure sensor measurements, together with inertial sensor measurements, to produce a unified PVT solution. Innovations-based measurement exclusion is applied to reduce the impact of GNSS and TRNS multipath errors and pressure anomalies due, e.g., to ground effect at take-off and landing. Both loosely- and tightly-coupled techniques are tested on an aerial vehicle platform in an environment where both GNSS and TRNS signals are available. Error growth of the tightly-coupled technique during extended intervals of GNSS denial is studied to determine whether UAM service could continue uninterrupted when only inertial and TRNS measurements remain available. [8] analyzes the fundamental trade-offs that occur in the co-design of orthogonal frequency-division multiplexing signals for both ranging (via time-of-arrival estimation) and communications. These trade-offs are quantified through the Shannon capacity bound, probability of outage, and the Ziv-Zakai bound on range estimation variance. These bounds are derived for signals experiencing common impairments, Rayleigh fading, and multipath channels. Using these bounds, analysis is provided demonstrating how Pareto-optimal design choices can be made to optimize the communication throughput, probability of outage, and ranging variance. Furthermore, different signal design strategies are analyzed, showing how certain designs achieve better performance depending on the channel.

Traditional Global Navigation Satellite System (GNSS) immunity to interference may be approaching a practical performance ceiling. Greater gains are possible outside traditional GNSS orbits and spectrum. GNSS from low Earth orbit (LEO) has long been viewed as promising but expensive, requiring large constellations for rapid navigation solutions. The recent emergence of commercial broadband LEO mega-constellations invites study on dual-purposing these for both communications—their primary mission—and a secondary PNT service [9]. Operating at shorter wavelengths than traditional GNSS, these constellations would permit highly directive, relatively compact receiver antennas. PNT-specific on-orbit resources would not be required: the transmitters, antennas, clocks, and spectrum of the hosting broadband network would suffice for PNT. Non-cooperative use of LEO signals for PNT is an option, but cooperation with the constellation operator ("fusion" with its communications mission) eases the burden of tracking a dense, low-altitude constellation from the ground and enables a receiver to produce single-epoch stand-alone PNT solutions. This paper proposes such a cooperative concept, termed fused LEO GNSS. Viability hinges on opportunity cost, or the burden a secondary PNT mission imposes on the communications constellation operator. This is assessed in terms of time-space-bandwidth product and energy budget. It is shown that a near-instantaneous-fix PNT service over $\pm 60^{\circ}$ latitude (covering 99.8% of the world's population) with positioning performance superior to traditional GNSS pseudoranging would cost less than 1.6% of downlink capacity for the largest of the new constellations, SpaceX's Starlink. This allocation is comparable to adding one user consuming 5.7 Msps of broadband service to each cell. Traditional GNSS has been brilliantly successful, yet for some applications, they remain inadequate with regard to the accuracy, constellation survivability, or robustness to interference—for both civil and military users. To address these limitations, several alternative augmentation systems have been investigated. In this context, GNSS augmentations are defined as sensors other than GNSS receivers or IMUs that can be used for PNT. Potential GNSS augmentations are cameras, radars, lidars, terrestrial radio navigation systems (TRNS), communication systems, LEO PNT, and other signals of opportunity. These alternate sensors can operate as both supplements to GNSS, as well as stand-alone PNT solutions in GNSS-denied environments. This section covers GNSS augmentations in the following order: (1) Vision-based; (2) Radar-based; (3) TRNS; (4) Communication systems; (5) LEO PNT; and (6) Signals of Opportunity.

2.2.1 Vision:

On vision systems, Petit et al. were the first to discover a camera blinding attack by laser shooting, which was demonstrated on MobilEye [87]. Yan et al. further demonstrated such attacks via both laser shooting and LED light shooting [88]. However, these works were focused on sensing mechanism-specific attacks and did not take a close look at potential vulnerabilities on the downstream AI perception algorithm side. For the latter, various works have studied physical-world attacks (e.g., using malicious stickers/patches/posters) against camera-based perception and localization algorithms in HAV context, e.g., those for traffic sign detection [89, 90, 91, 92, 93], object tracking [94], lane detection [95, 96, 97], multi-sensor fusion [98], vehicle detection [92, 99], pedestrian detection [100, 101], etc. Among them, several recent works were able to demonstrate the attack effectiveness on commercial HAV systems, such as a commercial traffic sign recognition system [93] and commercial lane keeping systems [95, 96]. Besides using stickers/patches/posters, several prior works also found that projectors can be used to attack camera-based HAV perception algorithms as well, e.g., by projecting patterns to the ground [102] or to the traffic sign surface [103]. Besides using physical-world attacks, several works also explored using sensor attacks to attack the camera perception, e.g., using GPS spoofing [104] and laser shooting [105] to attack traffic light detection, using invisible infrared lights (IR light) to attack object detection and localization [106], and using projector light shooting to attack traffic sign detection [107].

Micro aerial vehicles (MAVs) are increasingly being used for applications such as 3D mapping that requires both (1) precise pose (position and orientation) knowledge relative to a global coordinate system fixed to the Earth's surface, and (2) close-in maneuvers to ensure high resolution of the area being mapped. A global coordinate system is essential for applications such as automated infrastructure inspection[108], 3D modeling of buildings [109], disaster recovery or search and rescue[110], and open-world virtual reality [74], in which mapping data from the MAV is consumed by other, possibly automated, agents, potentially long after the initial mapping process.

Carrier-phase differential GNSS (CDGNSS) techniques such as real-time kinematic (RTK) positioning can offer centimeter-accurate positioning accuracy, and so serve as an excellent anchor for globally-referenced pose estimation. However, such accuracy is only achieved robustly and instantaneously when so-called carrier phase ambiguities are resolved to their integer values [111]. Confident ambiguity resolution depends on a large number (e.g., 12+) of participating low-multipath GNSS signals[112], or on a tight prior position estimate. But as a mapping MAV passes close to buildings, under overhanging rooftops, or around foliage, GNSS signal blockage and multipath effects become severe, limiting the availability of CDGNSS unaided by inertial sensing. Users of mapping MAVs therefore currently tend to avoid altogether areas where GNSS signals might be obstructed [113].

The MAV platform also places unique constraints on navigation systems: onboard compute is restricted by size, weight, and power limitations; the lively system dynamics of MAVs require low-latency measurement and estimation; and, in many cases, MAVs may only feature low-cost consumer-grade cameras and inertial measurement units (IMUs).

[73] describes a method for improving CDGNSS performance via tight coupling with a visual-inertial pose estimator. A CDGNSS system is defined herein as *tightly coupled* with visual and inertial sensing if the latter aid in resolving CDGNSS integer ambiguities. A *loosely coupled* CDGNSS system, in contrast, is based on a standalone CDGNSS estimator that operates without aiding other sensors. Information in a loosely-coupled system only flows one way, from the CDGNSS estimator to the downstream estimators.

Tight coupling with inertial sensors is a widely-studied and well-understood method of increasing the robustness and availability of fixed-integer CDGNSS positioning [39, 40, 41, 42]. Early efforts used high-quality navigation- or tactical-grade inertial sensors to provide positioning constraints over lengthy GNSS outages. More recently, researchers have exploited lower-cost industrial-grade micro-electro-mechanical system (MEMS) inertial sensors to bridge short GNSS outages [114, 115, 43] or for attitude-only CDGNSS [71]. These industrial-grade MEMS sensors are significantly larger, heavier, and more expensive than the consumer-grade MEMS inertial sensors of the type commonly found in low-cost MAVs.

In a companion paper[74], tight coupling with a consumer-grade MEMS sensor is shown to improve CDGNSS performance in degraded GNSS conditions or over short complete outages. The current paper explores the addition of visual measurements to the same tightly-coupled inertial-CDGNSS system analyzed in [74].

There are reasons beyond integer ambiguity fixing for inertial sensing in precise MAV positioning: First, CDGNSS combined with an inertial sensor can provide the full pose of the vehicle. Second, inertial sensing allows the global the scale of visual features to be observable when combined with visual positioning, which is important for visual-inertial positioning during GNSS outages [116].

A popular method for MAV navigation is the fusion of visual and inertial measurements [117, 118, 119, 120, 121]. These systems generally operate by tracking visual features seen by one or more cameras, and taking the position of features in the camera field of view as measurements for a pose estimator [117]. In some cases, the positions of the visual features are jointly estimated along with the camera pose, in a technique known as simultaneous localization and mapping (SLAM). Absent a prior globally-referenced map, visual-inertial navigation systems are fundamentally relative positioning systems, and cannot provide a globally-referenced pose estimate. They also suffer from odometric drift except in certain cases where returning to a previously-visited location enables "loop closure."

Tight coupling of visual-inertial sensing with CDGNSS has not been as widely studied as inertial-only coupling. The VISRTK technique proposed in [47] directly incorporates the double-difference carrier phase measurement model, including integer ambiguities, into a bundle-adjustment based SLAM problem. This approach is near-optimal, but far too computationally demanding for real-time implementation on an MAV, and does not attempt to incorporate IMU measurements.

The authors of [122] proposed tight coupling of CDGNSS with visual positioning, an inertial sensor of unstated quality, and barometric altitude measurements, but the visual positioning method used requires the collection and curation of precise aerial imagery. The use of 2-dimensional aerial maps also precludes close-in maneuvering to buildings and other obstacles.

Li et al. in [123] implemented tight coupling of single-antenna CDGNSS with monocular visual-inertial odometry via a multi-state constraint Kalman filter (MSCKF) [119]. However, the system as reported depended on an industrial-grade IMU. Moreover, SLAM-type visual-inertial techniques can be advantageous over MSCKF estimation due to their ability to map visual features while an RTK fix is available, then exploit the previously-mapped features during an outage. In contrast, the MSCKF technique is fundamentally odometric: visual feature tracks are immediately marginalized when ingested into the filter.

The work perhaps most comparable to this paper is [124], which describes the tight coupling of CDGNSS, a smartphone-grade IMU, SLAM-based visual feature measurements, and a beacon-based local positioning system for a robotic lawn mower application. While [124] showed that visual measurements reduce the overall position drift during an RTK fix outage, it did not offer a convincing demonstration of an improved integer fix rate.

The primary contribution of [73] is the incorporation of visual measurements into a tightly-coupled multi-antenna CDGNSS-inertial pose estimator using a smartphone-grade IMU and camera. It provides the first demonstration of an increased RTK integer fix rate using visual-inertial aiding with smartphone-grade sensors.

2.2.2 Radar

Due to the fundamental role of RADAR, LiDAR, and vision systems in HAV systems, various prior works have studied their security issues in HAV contexts, especially those under the more realistic external physical-layer attack models (e.g., sensor/analog attacks). On RADAR, Yan et al. are the first to show jamming and spoofing attacks on the millimeter-wave RADAR on Tesla Model S, with the former able to make detected objects disappear from the Autopilot system, and the latter able to alter the object distance [88]. Sun et al. performed a more comprehensive follow-up analysis, which was able to show more reliable spoofing effects and the ability to cause meaningful system-level effects (e.g., vehicle crashes) to the victim HAV [125].

The development of automated ground vehicles (AGVs) has spurred research in lane-keeping assist systems, automated intersection management [37], tight-formation platooning, and cooperative sensing [126, 127], all of which demand accurate (e.g., 50-cm at 95%) ground vehicle positioning in an urban environment. But the majority of positioning techniques developed thus far depend on lidar or cameras, which perform poorly in low-visibility conditions such as snowy whiteouts, dense fog, or heavy rain. Adoption of AGVs in many parts of the world will require all-weather localization techniques.

Radio-wave-based sensing techniques such as radar and GNSS (global navigation satellite system) remain operable even in extreme weather conditions because their longer-wavelength electromagnetic radiation penetrates snow, fog, and rain. Carrier-phase-differential GNSS (CDGNSS) has been successfully applied for the past two decades as an all-weather decimeter-accurate localization technique in open-sky conditions. Proprioceptive sensors such as inertial measurement units (IMUs) also continue to operate regardless of external conditions. Coupling a CDGNSS receiver with a tactical-grade inertial sensor, as in [39, 40, 41, 42] delivers robust high-accuracy positioning even during the extended signal outages common in the urban environment, but such systems are far too expensive for widespread deployment on AGVs. Recent work has shown that 20-cm-accurate (95%) CDGNSS positioning is possible at a low cost even in dense urban areas, but solution availability remains below 90%, with occasional long gaps between high-accuracy solutions [30]. Moreover, the global trend of increasing radio interference in the GNSS bands, whether accidental or deliberate [81], underscores the need for GNSS-independent localization: GNSS jamming cannot be allowed to paralyze an area's automated vehicle networks.

Clearly, there is a need for AGV localization that is low cost, accurate at the sub-50-cm level, robust to low-visibility conditions, and continuously available. [53] is the first to establish that low-cost inertial- and automotive-radar-based localization can meet these criteria.

Mass-market commercialization has brought the cost of automotive radar down enough that virtually all current production vehicles are equipped with at least one radar unit, which serves as the primary sensor for adaptive cruise control and automatic emergency braking. But the use of automotive radar for localization faces the significant challenges of data sparsity and noise: an automotive radar scan has a vastly lower resolution than a camera image or a dense lidar scan, and is subject to high rates of false detection (clutter) and missed detection. As such, it is nearly impossible to deduce semantic information or extract distinctive environmental features from an individual radar scan. The key to localization is to aggregate sequential scans into a batch, where environmental structure is clearly evident. Even still, the data remain so sparse that localization based on traditional machine vision feature extraction and matching is not promising. Additionally, stable short-term odometry is a pre-requisite for aggregating radar scans, which in itself is a challenge when dealing with low-cost inertial sensing.

[53] proposes a two-step process for radar-based localization. The first is the mapping step: the creation of a geo-referenced two-dimensional aggregated map of all radar targets across an area of interest. The full radar map used throughout [53], was constructed with the benefit of a highly stable inertial platform so that a trustworthy ground truth map would be available against which maps generated by other techniques could be compared. But an expensive inertial system or dedicated mobile mapping vehicle is not required to create a radar map. Instead, it can be crowd-sourced from the very user vehicles that will ultimately exploit the map for localization. During periods of favorable lighting conditions and good visibility, user vehicles can exploit a combination of low-cost CDGNSS, as in [30], and GNSS-aided visual simultaneous localization and mapping, as in [38], to achieve the continuous decimeter-and-sub-degree-accurate geo-referenced position and orientation (pose) required to lay down an accurate radar map. In other words, the radar map can be *created* when visibility is good and then *exploited* at any later time, such as during times of poor visibility.

Despite aggregation over multiple vehicle passes, the sparse and cluttered nature of automotive radar data is evident from the radar map: the generated point cloud is much less dense and has a substantially higher fraction of spurious returns than a typical lidar-derived point cloud, making automotive-radar-based localization a significantly more challenging problem.

The second step of [53]'s technique is the localization step. Using a combination of all-weather odometric techniques such as inertial sensing, radar odometry, and ground vehicle dynamics constraints, a sensor fusion filter continually tracks the changes in vehicle pose over time. Over the latest short interval (e.g., $5\,\mathrm{s}$), pose estimates from the filter are used to spatially organize the multiple radar scans taken over the interval and generate what is hereafter referred to as a batch of scans, or batch for short. In contrast to the individual scan, some environmental structure emerges in the batch of scans, making robust registration to the map feasible. Even so, the localization problem remains challenging due to the dynamic radar environment: note the absence of parked cars on the left side of the street during localization. The batch of scans is matched against the prior map of the surroundings to estimate the pose offset of the batch from the truth. This pose offset is then applied as a measurement to the sensor fusion filter to correct odometric drift.

[53] contributes a robust pipeline for all-weather sub-50-cm urban ground vehicle positioning. This pipeline incorporates a computationally-efficient correlation-maximization-based globally-optimal radar scan registration algorithm that estimates a two-dimensional translational and a one-dimensional rotational offset between a prior radar map and a batch of current scans. Significantly, the registration algorithm can be applied to the highly sparse and cluttered data produced by commercially-available low-cost automotive radars. The maximization of correlation is shown to be equivalent to the minimization of the L^2 distance between the prior map and the batch probability hypothesis densities. The pipeline supports the construction of the radar registration estimate and optimally fuses it with inertial measurements, radar range rate measurements, ground vehicle dynamics constraints, and cm-accurate GNSS measurements, when available. A novel technique for online estimation of the vehicle center of rotation is introduced, and calibration of various other extrinsic parameters necessary for optimal sensor fusion is described.

A thorough evaluation of the positioning pipeline on the large-scale dataset described in [31] is presented. Data from automotive sensors are collected over two $1.5\,\mathrm{h}$ driving sessions through the urban center of Austin, TX on two separate days specifically chosen to provide variety in traffic and parking patterns. The dataset is collected in clear weather conditions, but only includes data from sensors that are expected to remain unaffected in adverse weather. Comparison with a post-processed ground truth trajectory shows that proposed pipeline maintains 95^{th}-percentile errors below $35\,\mathrm{cm}$ in horizontal position and $0.5°$ in heading during $60\,\mathrm{min}$ of GNSS-denied driving.

2.2.3 Lidar

On LiDAR, Petit et al. is the first to show that laser shooting can be used to inject spoofed points into a commercial LiDAR [87]. Shin et al. improved the attack mechanism to achieve spoofed point injection at a closer distance than the LiDAR device, and also designed the first jamming attack against LiDAR [128]. Building upon it, Cao et al. are the first to achieve successful near-front vehicle spoofing at LiDAR object detection model level and also end-to-end system-level attack effect (e.g., emergency brake) in an industry-grade HAV system [129]. They achieved it by systematically combining LiDAR spoofing and adversarial machine learning attack, dubbed “adversarial sensor attack”, which is the first sensor-AI co-designed attack in the CPS context. Sun et al. further designed a black-box version of such an adversarial sensor attack to improve the attack practicality and generality [130]. They further designed the first principled defense method against such attacks by using physical invariants from LiDAR sensing mechanism, which was able to both detect attacks without modifying models and harden models, both without hurting accuracy since such invariants should also hold in benign cases [130]. After that, Hallyburton et al. found that camera-LiDAR fusion algorithms can by nature have defense capabilities against LiDAR spoofing, and were able to further design a new attack to systematically bypass such fusion-based defense [131]. Most recently, Cao et al. discovered that spoofing attacks can also be used to remove points by moving the points in a range all to the LiDAR Minimum Operational Threshold (MOT), which were able to show the removal of $\sim$4,000 point [132].

Besides sensor attacks against LiDAR, there also exist several physical-world attacks discovered against LiDAR, mainly using adversarial 3D objects. Specifically, Cao et al. were the first to discover that maliciously-shaped 3D objects can be used to attack both camera and LiDAR object detection in HAV context while maintaining high stealthiness (e.g., by mimicking normal road objects such as traffic cones and rocks) [98]. They were also able to concretely demonstrate their attack effect in the physical world using a real HAV vehicle. Using the same attack vector, Yang et al. were able to design a new attack that use a small roadside object to spoof a vehicle [133]. Besides carefully-crafted adversarial 3D objects, simple objects (e.g., cardboard and road signs) are also found to be effective in attacking LiDAR perception [134, 135].

2.2.4 Terrestrial Navigation Systems

GNSS have provided excellent positioning solutions in open, outdoor environments, enabling a wide range of navigation and timing applications. However, the indoor environment remains largely out of reach to these weak signals. The requirement for accurate and assured indoor positioning limits the effectiveness of GNSS in high-stakes, safety-of-life applications like enhanced E911, as well as in a new generation of commercial applications like warehouse automation and asset tracking.

Terrestrial radionavigation systems (TRNS), such as the commercial systems Locata [136] and NextNav [137], are emerging to address these needs. These systems are marketed to provide position, navigation, and timing (PNT) solutions in environments where GNSS signals are degraded or denied. TRNS consist of networks of synchronized terrestrial transmitters, or *pseudolites*, which operate analogously to GNSS satellites. These pseudolites broadcast signals powerful enough to reach the interiors of typical buildings, permitting the acquisition of terrestrial PNT service by urban or indoor users. A TRNS may serve to augment GNSS signals, improving solution geometry and availability in dense urban areas [138, 139], or it may serve as a primary navigation aid in the indoor environment [140].

The TRNS architecture [136, 137] and its sensitivity to wide-band radio-frequency interference (RFI) [141, 142] have been investigated in the literature. There have not, however, been any public proposals for how to secure TRNS–or even any substantive discussion of security considerations.

Broadly, the security of TRNS parallels that of other historical radio-navigation systems, and thus security considerations for TRNS can draw from lessons learned in the vibrant body of research on GNSS signal security. The important distinctions are threefold: first, the vastly different dynamic range of terrestrial versus space-based transmissions; second, the largely indistinguishable angular distribution of spoofed and authentic signals; and third, the possibility of multi-lateral (i.e. network) sensing of transmissions within the space bounded by the pseudolites. Of particular note is the way in which the adversary's receive power advantage renders exotic signal-level security techniques like spreading code authentication [143, 144] or deterministic code-phase dithering irrelevant: the adversary can always produce a pristine signal replica.

[7] analyzes the security considerations of TRNS with these three differences in mind. It offers a concrete proposal for how to secure TRNS, with a focus on data-level security in recognition of the futility of waveform- or signal-level security. This concrete proposal has two non-obvious aspects: MAC leavening, whereby a modest number of message authentication bits spread throughout the transmitted packets provide a significant improvement in security, and multi-level encryption, which has not been used before in PNT security and makes the adoption of this proposal more enticing for commercial service providers.

From the perspective of a radio-navigation system, there are essentially two types of adversaries: parties wishing to obtain service without authorization (stow-aways), and parties wishing to deny, degrade, or deceive authorized users of the service (jammers or spoofers). This divides radio-navigation security into two domains, termed Encryption (denying stow-aways) and Authentication (detecting spoofing). (N.B. that cryptographic encryption techniques are a useful tool in both domains). The focus of this work on terrestrial commercial systems prompts the adoption of the term "subscriber" to refer to an authorized user.

The greater dynamic range of terrestrial signals is a fundamental difference in the following sense: with GNSS, a spoofer cannot easily gain an advantage in received signal strength by moving closer to the transmitter, because this would require climbing thousands of kilometers above the ground. Instead, the adversary who wishes to obtain a pristine signal must build a large antenna. In TRNS, however, the adversary can "walk right up to" the pseudolite, obtaining a signal as clear as they could wish. Furthermore, because a subscriber cannot anticipate how much path loss may be present, it cannot anticipate how strong a signal ought to be after de-spreading. These asymmetries enable an adversary to obtain pristine signal replicas at low cost and high reliability, by locating a receive antenna close to the pseudo-lite. This renders spreading code encryption (SCE) (after the fashion of the GPS P(Y) code) largely irrelevant for TRNS: an adversary can always build a network of receivers to obtain both the pseudolites' spreading codes and position.

The threat from GNSS spoofing has been a concern within the GNSS community, ever since a portable spoofer was developed and successfully tested against a COTS receiver [145]. A number of live-signal spoofing tests in a controlled environment which followed thereafter also affirmed the effect [146, 147, 148]. This threat continues to be relevant today, with recent rumors of spoofing “in the wild” seen in specific spots such as Black Sea [149], Syria [150] and China [151], or affecting multiple victim receivers which coincidentally move along the same track [152]. With recent advancements in RF microelectronics, together with open-source GNSS signal generation software, building a functional GNSS spoofer will become more accessible to the masses in the near future [153]. The spoofing threat is also relevant to TRNS because a functional TRNS spoofer can be modified from a GNSS spoofer, given sufficient resources and knowledge of the TRNS signal architecture.

TRNS has differentiated itself by having a high SNR and a limited-access standard, which is perceived to be able to counter against conventional spoofers that rely on high signal power and accurate prediction of spreading code and/or navigation data bit to mount a successful attack. However, these characteristics do not make TRNS foolproof against all spoofing threats. In fact, TRNS system has to tackle additional challenges due to high signal strength, wider signal dynamic range, proximity of threats to transmitters, as well as a potential reliance on GNSS for network synchronization. TRNS therefore faces a longer list of vulnerabilities from its signal and physical characteristics than GNSS.

Unlike GNSS signals that have signal strength below noise floor, the spreading code sequence of TRNS can be exposed without the use of high-gain antenna due to its high SNR. Reference [154] shows that the time slot usage, transmitters’ PRN and navigation data bit of the Metropolitan Beacon System (MBS) from NextNav can be derived by analyzing the power spectrum of the MBS signal. This makes the cost of SCER attack on TRNS lower than that on GNSS, since the embedded security codes of TRNS can be more easily observed and hence estimated. In addition, even if TRNS adopts a restricted access standard and requires the use of secure tamper-resistant receiver to store the secret key like military GNSS signals, it is still susceptible to record-and-replay attacks.

TRNS provides a wide-area positioning service using a network of synchronized terrestrial transmitters. To ensure high accuracy in the PNT solution, stringent synchronization and frequency stability requirements are placed on all pseudolites, which may be satisfied either by: (1) the use of dedicated low-latency fiber-optic connection across the entire network, which will incur significant setup cost and will limit the deployment sites, or (2) the use of GNSS-disciplined atomic clocks, which reduces infrastructure cost and offers greater flexibility in the placement of the pseudolites. While option 2 may be preferable to providers, it exposes TRNS to an additional attack surface through its reliance upon GNSS. In addition, the relative accessibility of the pseudolites compared to the Earth-orbiting GNSS satellites indicates that TRNS is more susceptible to direct attacks, either by physical or cyber tampering, or by co-locating a high-power interference transmitter to overwhelm its signal.

TRNS inherits from traditional radio-navigation a bevy of well-known attacks. For the same reason, TRNS can benefit from the products of a vibrant research effort over the past 20 years to secure GNSS. Not all the techniques that have been proposed for securing GNSS are applicable to TRNS— but it is equally true that the obligation of GNSS operators to backwards compatibility has prevented them from fully exploiting these developments. The time is right to incorporate what has been learned about GNSS security into TRNS. The purpose of this section is to review some of the most powerful security techniques that have been proposed for GNSS and to identify those ideas that are compatible with TRNS.

GNSS spoofing defenses proposed in recent literature can be broadly classified into two categories: (1) cryptographic techniques that utilize unpredictable but verifiable signal modulation in the GNSS spreading code or navigation data, and (2) non-cryptographic techniques such as signal processing techniques, geometric techniques, or drift monitoring techniques. A comprehensive review of GNSS spoofing defenses is presented in [78]. While these techniques have been proven to be effective for GNSS, there are challenges to their implementation for TRNS. The preliminary ideas of GNSS spoofing defenses fall within the realm of non-cryptographic defenses, as they do not require any changes to GNSS signal-in-space (SIS). These techniques are categorized based on their method of differentiating spoofing signals from authentic signals, by looking for consistency in the signal characteristics, signal geometry, or PNT solution.

Geometric techniques exploit the RF signals' geometric diversity to verify the authenticity of the signal source. This includes angle-of-arrival (AOA) discrimination techniques [82, 65, 155, 156] or Doppler frequency difference of arrival (FDOA) [157] discrimination using multiple antennas. Other geometric techniques advocate the use of single antenna, and discriminate spoofed and authentic signals either with a known perturbation profile [158] or random motion profile [159], or using multiple feeds from a single antenna [160]. The assumptions made by these techniques are: (1) the spoofing signals generally arrive from below or near the horizon [160], (2) the observations from spoofing signals is not aligned with the actual geometry between the satellites and the victim receiver [82, 155], and (3) there are strong correlation of signal characteristics of different satellites from the spoofing signals [158, 65, 159, 156]. However, it is not costly for a sophisticated spoofer to co-locate dedicated spoofing sources at each of the TRNS pseudolites, thereby defeating all the assumptions made by these techniques. In addition, the need for hardware modification or additional hardware might not be suitable for applications that either use an existing hardware for mass-market adoption, or have SWaP-C constraints.

Drift monitoring techniques, on the other hand, look for unusual changes in the output of the receiver, such as position or clock fix, by coupling with external sensors. These include the use of an oscillator to check for inconsistency in the clock bias or clock drift [161], or the use of visual/inertial/radar odometry to place constraints on the reasonable error growth of a position fix [162, 163]. The applicability of these techniques is limited by the SWaP-C constraints of the applications, and the authentication performance is limited by the accuracy of these sensors.

Signal processing techniques look for sudden deviations in the received signal characteristics to indicate an onset of a spoofing attack. These techniques detect changes in the received carrier amplitude or the RF front-end's AGC set-point, or a distortion in the complex correlation function [164]. Signal processing techniques can be implemented in software, unlike the previous categories of techniques discussed which require additional hardware. These techniques are effective for GNSS which has signal strength below the noise floor and narrow signal dynamic range. However, this is not applicable to TRNS, which generally has high SNR and a wide signal dynamic range for quick acquisition in both dense-urban and indoor environments. A potential spoofer will have a wide margin to change the total received power and create a distortion-free correlation function using the spoofing signal, and these indicators will not be picked up by the PD detector proposed by [164].

The main objective of cryptographic spoofing defenses is to ensure information security. Cryptographic techniques include encryption, which enforces the secrecy of data from unauthorized access, and authentication which verifies the origin of the data. They provide three features: (1) authentication, by verifying the origin of information, (2) confidentiality, by protecting the information from disclosure to non-authorized parties, and (3) integrity, by detecting any unauthorized information modification. These features increase the resilience of the signal against spoofing.

Several GNSS cryptographic spoofing defenses have been proposed and/or implemented in both civil and limited-access GNSS signals. These spoofing defenses add cryptographic features in small segments or in entire portion to either the fast-rate spreading code or the low-rate navigation data. These cryptographic techniques can be classified into the following groups: (1) navigation message encryption (NME), which encrypts the whole navigation data message before being modulated onto the spreading code, (2) spreading code encryption (SCE), which encrypts the whole spreading code sequence, (3) navigation message authentication (NMA), which adds unpredictable digital signature into the navigation data using asymmetric cryptography, and (4) spreading code authentication (SCA), which inserts unpredictable watermark sequences within the open spreading code.

The straightforward, blanket encryption of a navigation signal may be attractive as a means both to deny service to stow-aways and to authenticate the signal to subscribers. However, there are sigificant caveats in both applications. The first regards the use of symmetric cryptography.

One may apply symmetric encryption to the entire navigation message (NME) and/or the spreading code (SCE, *a la* the GPS P(Y) code). The premise is that a spoofer who does not know the symmetric key cannot produce a valid spoofing signal, or equivalently that a receiver can be confident in a signal that appears in the output of a correlator tuned to the secret spreading sequence (with similar reasoning for NME). However, a symmetric approach to authentication is extremely fragile, because a leaked symmetric key can be used for spoofing. For this reason, military deployment of SCE involves tamper-resistant hardware and costly, elaborate procedures for secure distribution and management of the secret symmetric keys. This approach is untenable for civil or commercial radio-navigation.

NMA and SCA, in contrast, avoid the fragility of symmetric key management by adopting asymmetric cryptography, using either delayed release approach or public-private key pair. In SCA, short segments of unpredictable spreading code sequences (termed as "watermarks") are interleaved with long segments of predictable spreading codes in fixed or random positions [143]. The receiver uses the predictable sequences to track the broadcast signal, and stores the unpredictable segments in the buffer while waiting for the information about the watermarks. Once this information arrives, the receiver can synthesize the unknown spreading sequence with the correct watermarks embedded in the right position, and correlates this code segment with the relevant segment from its recorded signal to verify signal authenticity. This technique requires modifications to the GNSS signal generation. Hence, it will be difficult or impossible to be implemented on existing GNSS which requires backward compatibility. However, TRNS, which comes with a green-field waveform, can consider the implementation of SCA into its waveform design.

A growing literature advocates the use of NMA for civil GNSS signal authentication, with proposed implementations for GPS [143, 165, 166], Galileo [167, 168], QZSS [169] and SBAS [170, 171, 172]. NMA is already implemented in the Galileo Open Service, which will start its Open Service Navigation Message Authentication (OSNMA) signal-in-space transmission in the first quarter of 2020 and have full service available in 2021 [173]. This technique uses either an asymmetric private-key/public-key approach such as the *elliptic curve digital signature algorithm* (ECDSA) [166], or a delayed symmetric key release approach such as *timed efficient stream loss-tolerant authentication* (TESLA) [165]. Unlike SCA, this technique can be implemented into existing GNSS signal, provided that there are available unused bits in the navigation message to store the digital signature. However, the leftover bits in the navigation message are usually limited. A trade-off has to be made between the cryptographic strength of the NMA scheme, which is determined by the size of the key and the digital signature, and the authentication latency, which is determined by the frequency of digital signature validation. TRNS has more flexibility in incorporating NMA into their waveform design, and can offer low *time-to-first-authenticated-fix* (TTFAF) while maintaining strong cryptographic security.

In contrast to GNSS, TRNS comes with a clean-slate waveform design, and is not constrained by the need of backward compatibility. This offers TRNS providers flexibility in their application of the latest cryptographic defense techniques—many of which were originally proposed for GNSS. The next section proposes one implementation of NME and NMA for a TRNS.

As recently outlined in [7], however, TRNS have unique security challenges: (1) the dynamic range of TRNS signal power is vastly wider than that of GNSS, allowing would-be spoofers access to high signal-to-noise ratio (SNR) signals and complicating spoofing mitigation based on simultaneous demodulation of spoofed and authentic waveforms [174]; (2) the angular distributions of spoofed, authentic, and multipath signals significantly overlap, rendering angle-of-arrival techniques based on multi-element antennas [65, 175] less effective; and (3) TRNS transmitters are physically accessible.

Nevertheless, TRNS also have inherent security advantages. Chief among these is that TRNS transmitters also function as receivers and can thus (1) accurately characterize the surrounding signal landscape's nominal statistics and thereafter (2) search for anomalies that reveal the presence of interfering signals. Current development of commercial TRNS clean-slate designs offers an opportunity to exploit this advantage of TRNS for enhanced security. The present work complements the cryptographic security proposal presented in [7]. Briefly, [7] proposes a multi-tiered navigation message encryption (NME) + message authentication code (MAC)-based navigation message authentication (NMA) scheme. One can think of [7] as offering a basic level of navigation security via cryptographic methods. No TRNS should be fielded without such basic measures.

However, the techniques proposed in [7] are not sufficient to secure TRNS because the exposed spreading codes of a high-SNR TRNS signals makes them vulnerable to replication in a security code estimation and replay (SCER) [176] or meaconing attack. More generally, NME+NMA cannot fully protect TRNS against low-latency replay attacks. Even exotic signal-level security techniques like spreading code authentication (SCA) [144] or deterministic code-phase dithering [177] can be rendered ineffective by a spoofer's ability to access high-power authentic signals in a TRNS network. To address the gap in TRNS defenses against low-latency signal replay attacks, [6] proposes an autonomous signal-situational-awareness (SSA) overlay capability within a TRNS network. SSA is intended to augment basic TRNS cryptographic security. While some spoofers will remain undetectable, SSA gives TRNS operators a significantly improved chance of catching threats and alerting users without resorting to costly full-duplex techniques (those requiring bi-directional communication with users). Note that SSA is not possible for current GNSS space vehicles in medium Earth orbit, which can neither receive each other's signals nor detect low-power ground-based spoofers. [6] seeks to place TRNS SSA on a solid theoretical and practical footing. First, signal authentication techniques for SSA are developed based on the prior work in [79] and [80]. Second, simulations with a theoretical model of multipath and spoofing signals are used to quantify the effectiveness of autonomous SSA under some of the myriad operating conditions encountered by generic TRNS.

Central to the transportation revolution that will be driven by urban air mobility (UAM) is the problem of robust and secure navigation. Urban environments offer more challenges, such as interference and multipath, when compared to open-sky conditions. As the only positioning system that offers absolutely-referenced meter-level accuracy with global coverage, GNSS will no doubt play a significant role in this revolution. If strengthened against jamming and spoofing, carrier-phase-differential GNSS (CDGNSS), coupled with low-cost inertial sensing, will be nearly sufficient for position, velocity, and timing (PVT) needs. But nearly sufficient is insufficient: it is not enough for a UAM PVT solution to offer decimeter-accurate positioning with 99% availability, or even 99.9% availability. UAM will demand that its navigation systems offer dm-accurate positioning with integrity risk on the order of 10^{-7} for a meter-level alert limit and availability with several more 9s than 99.9% [178, 179, 52, 180].

[5] technique is best viewed as one part of a comprehensive navigation solution concept called deep-layered navigation (DLN) in which synergistic but independent navigation systems are layered to increase accuracy and robustness. DLN is the navigation analog of the "defense in depth" concept in information security, where multiple layers of security

controls and checkpoints are emplaced throughout a system such that even when some layers are breached, security is maintained. Likewise, in the safety-of-life UAM navigation context, multiple layers of navigation systems, all interoperable and mutually-reinforcing but substantially independent, are an essential defense against the whims of Mother Nature and the foibles of human nature.

At DLN's core sits redundant inertial navigation, which is virtually impervious to radio frequency (RF) interference, poor weather, signal blockage, and data ambiguity. The outermost layer—the default navigation system and first line of defense—is a specialized variant of inertially-aided CDGNSS, recently developed in [3, 4], that has been substantially secured against spoofing and substantially hardened against the multipath and signal blockage conditions of the urban *ground vehicle* environment, which can be considered a worst-case realization of the urban air vehicle environment. But despite its coupling with inertial sensing, the technique developed in [3] cannot tolerate extended GNSS outages. A secondary source of absolute PVT is required to bound the growth of position errors.

TRNS beacons provide much stronger signals compared to GNSS, operate at a different frequency, and offer a full absolutely-referenced backup PVT solution to GNSS. In particular, [5] explores tight coupling with NextNav's Metropolitan Beacon System (MBS). MBS is particularly attractive for UAM because its signals carry not only wideband (multipath-resistant) synchronization sequences for ranging but also corrections data for barometric altitude determination and, for CDGNSS. [5] presents the development of a tightly-coupled GNSS-TRNS-inertial PNT system is a prelude to upcoming work on comprehensive deep-layered navigation for UAM, including additional layers based on radar localization, visual odometry, and LEO-satellite-provided GNSS.

Augmentation of GNSS with terrestrial signals has been explored and shown to provide an added benefit over exclusive use of GNSS [181, 182]. But these techniques were demonstrated only on ground vehicles, and the sensor integration with CDGNSS was not tightly-coupled: the terrestrial signals were not incorporated in a way that permitted aiding of the ambiguity resolution process critical to CDGNSS. Loose coupling between GNSS and TRNS has been used to augment GNSS and provide an increase in both accuracy and availability on aerial vehicles [183, 184, 185]. But these methods fuse standard GNSS, not CDGNSS, with TRNS, and thus lack the decimeter accuracy that will be desirable, if not required, for UAM. Relative ranging measurements from ultra wide band (UWB) systems have been used to constrain integer ambiguities in CDGNSS and improve accuracy even with degraded GNSS reception [186]. Although UWB systems provide adequate performance, the limited range of the UWB signal makes it an unfavorable choice for UAM. Fusion of GNSS and signals of opportunity has been explored for aerial vehicles with promising results [187, 188]. But for a safety-of-life application like UAM, it is likely that signals of opportunity will be viewed less favorably than a dedicated TRNS as a secondary means of navigation.

[5] makes four primary contributions. First, it presents and demonstrates the first use of tightly-coupled CDGNSS, TRNS, and inertial sensing to provide a secure and robust PVT solution. Second, it develops a novel innovations-based measurement exclusion

technique which mitigates the impact of GNSS and TRNS multipath errors and pressure anomalies. Third, it offers a comparative analysis of loose and tight coupling on an aerial vehicle in an environment where only TRNS signals are available. Fourth, it preforms a study of error growths during periods of GNSS denial to determine whether PVT requirements for UAM could be met despite extended intervals of GNSS denial.

2.2.5 Communication Systems

Today's wireless communication networks are experiencing an ever growing demand for not only traditional communications but accurate user positioning as well. As user-equipment (UE) continues to be deployed in increasingly mobile applications, ranging from automotive vehicles to aerospace markets, the next generation of wireless networks will need to keep up with high demands for precise positioning. Orthogonal frequency-division multiplexing (OFDM), which is the most commonly used modulation in today's cellular networks, has been adopted in the 802.11, long term evolution (LTE), and 5G new radio (NR) standards. While these OFDM-based standards currently include positioning protocols [189, 190], the standards designed these positioning protocols as a secondary priority to traditional communications, which prioritizes data rates, latency, and network reliability. Furthermore, non-cooperative users may attempt to extract ranging estimates without establishing a communication link within the network at all, instead using the communications as a signal of opportunity. In both cases, the existing OFDM signals are not designed to provide the most precise ranging estimates possible and may soon become insufficient to meet the markets precise positioning demands. To keep up with the importance of positioning, OFDM communication waveforms should be purposefully co-designed to prioritize both ranging and communications.

Envision a scheme where a UE attemps to determine its position without network cooperation. The most simple approach the UE can take is to correlate its received samples against the known portion of the signal: the training sequences and pilots. Through this correlation, the UE can extract a time-of-arrival (TOA) estimate and therefore a pseudorange measurement. Much like traditional GNSS processing, the UE can determine its location using pseudoranges from multiple base stations. However, this requirement to collect pseudoranges from multiple base stations runs almost contrary to the typical layout of wireless network cells: where regions are typically served by single base stations. As a result, the SNRs of signals collected from more distant base stations may be poor and possibly low enough that meaningful data cannot be transmitted over the link. At such low SNRs, TOA estimates experience a thresholding effect where the variance of TOA estimates rises dramatically. This phenomenon occurs when sidelobes in the autocorrelation function become the dominant source of estimation error, which will be referred to as the "sidelobe-dominated regime". As the SNR drops significantly low, the threshold plateaus in an "ambiguous regime", where meaningful estimates cannot be obtained from the signal and the best estimator is that which maximizes the prior belief about the TOA. As SNR increases, the thresholding effect in the sidelobe-dominated regime becomes less impactful and ultimately negligible, where the estimator enters a "mainlobe-dominated regime".

In this regime, the dominant source of error is from estimates that occur near the peak of the mainlobe in the signal's autocorrelation function. This mainlobe-domainated regime is precisely what the Cramer-Rao Lower Bound (CRLB) analyzes.

An additional regime may occur if the UE uses a more advanced approach than simply correlating against known pilots, especially when the SNR is high enough that data can be decoded. Some of these tecniques are included in 5G NR such as round-trip time and uplink-based TDOA but require cooperation with the network and the base stations. A new non-cooperative TOA estimation method, which prior work has not yet studied, is a decision-directed estimator. In this decision-directed approach, the UE would first decode the data bits carried in the data subcarriers, reconstruct the OFDM signal using these estimates, and correlate against the reconstructed signal rather than simply the known portion of the signal. Since data symbols make up a significant portion of the energy in OFDM transmissions, such a decision-directed estimator could experience noticeable gains in post-correlation SNR and a decrease in TOA estimation errors. A potential downside to this method is that incorrectly decoded bits could hinder the estimator and result in poorer performance. Therefore, the bit error rate would need to be low enough that the gains from correctly decoded bits outweigh degradation from incorrectly decoded bits. Above some SNR, this required error rate will become achievable, allowing the estimator to operate in a new decision-directed regime with enhanced positioning accuracy. Decision-directed approaches have seen success in channel and doppler estimation [191, 192], but so far have not been extended to range estimation for positioning. [8] focuses on the scheme where range is estimated through correlating only the known portions of an OFDM signal. The decision-directed scheme will be reserved for future work.

[8] explores how the design of OFDM signals impacts both range estimate precision and communication capacity in different propagation environments. To quantify ranging precision in these regimes, [8] makes use of the Ziv-Zakai bound [193]. The use of this bound as opposed to the CRLB is especially important as it captures the thresholding effects that occur in the sidelobe-dominated regime, which are entirely missed by the CRLB. To quantify capacity, Shannon capacity is computed, factoring in impairments due to multipath, block fading, carrier-frequency offset estimation error, and common phase errors. The design of these OFDM signals is dictated by several parameters, most importantly the placement and power allocation of pilots and training symbols throughout a single OFDM block. Furthermore, system requirements may be imposed on other parameters such as the subcarrier spacing, bandwidth, and cyclic prefix length. The selection of these parameters results in intricate tradeoffs between ranging precision and communication capacity, especially when channel impairments are considered. [8] quantifies these tradeoffs and proposes OFDM design solutions that balance performance in both ranging and capacity.

[8] derives the Shannon capacity bound and probability of outage for generic OFDM signals, accounting for channel estimation error, intercarrier interference, and common phase errors. Furthermore, [8] derives the Ziv-Zakai bound on range estimation variance for the same signals. These bounds also account for Rayleigh fading and multipath channels. [8] also proposes a method of co-designing OFDM signals to achieve both ranging and communication performance requirements through the use of Pareto curves plotting either the

Shannon capacity or probability of outage against the Ziv-Zakai bound on ranging error variance. These curves allow optimal system configurations to be selected. [8] analyzes how different channel impairments, fading models, and multipath impact both communications and ranging performance, demonstrating how certain signal designs are better suited for certain propagation environments than others.

Prior work has studied how OFDM signals can be used for positioning, but the majority of this work operates only within existing protocols rather than proposing new signal designs. This is a broad field of work, covering several protocols of interest. Time-of-arrival and ranging estimators for LTE signals have been analyzed in [194, 195, 196]. The Cramer-Rao Bound for TOA/range estimation is derived in both [195, 196] to evaluate the performance of their estimators. This bound has limited applicability in low SNR regimes. A comparison between OFDM and pseudonoise-based signals in [197] demonstrated that OFDM signals may provide improved time-based range estimation performance. A large number of publications have also focused on the field of opportunistic positioning and navigation, utilizing signals from LTE [198], FM OFDM [199], and mobile TV [200, 201]. While these studies provide valuable insights into the performance capabilities of such estimation and positioning algorithms, they do not necessarily address the design of the signals themselves, instead working within existing protocols.

Some work has specifically addressed the design of OFDM signals for ranging. Driusso et al. partially addressed signal design and studied how the placement of positioning pilots within the LTE framework affected ranging performance by computing the Ziv-Zakai bound [202]. But, while insights regarding subcarrier placement are valuable for the design of OFDM waveforms for ranging, the restriction to only signals achievable within LTE limits that study's applicability. Furthermore, the bounds discovered in [202] do not account for fading effects, which are common and known to degrade ranging performance. Wang et al. provided ranging accuracy bounds for a generic OFDM signal model that included multipath fading but only computed the CRLB, failing to address the SNR threshold effect, which will not be uncommon in OFDM-based ranging [203]. The study in [204] proposed a unique OFDM design strategy for selecting a sparse subset of bands to use in the signal such that time-delay estimation can meet set requirements under multipath propagation environments. The multipath signal modeling is rigorous and the estimation computationally complexity is significantly reduced using the proposed sparse design. However, the criterion used for optimization is the CRLB which ignores sidelobes and thresholding effects at low SNR. Furthermore, the study does not directly address how such a ranging signal would coexist within an OFDM system being used for communications as well. Another optimization technique is proposed in [205], in which pilots are allocated to optimize for both time-delay and channel estimation. Much like the previous paper, the CRLB is used in the optimization criterion limiting this techniques applicability in low SNR, and communication capacity is not factored in. Karisan et al. also took a similar approach [206] where an the power allocation across pilots was designed to minimizes the range estimation CRLB in the presence of interference. Similarly, [8] does not address low SNR thresholding effects or the tradeoffs that such a design would have with a joint communication system. While not specifically addressing OFDM design for ranging, the impact of

OFDM design parameters on sidelobe energy in the signal's autocorrelation function was analyzed in [207].

The communication capacity of OFDM systems has also been extensively studied in prior work. Goldsmith's textbook on wireless communications thoroughly covers the computation of channel capacity and outage in the presence of fading [208]. Yoo and Goldsmith extended this analysis to MIMO channels that have channel estimation error [209]. Tang et al. analyzed the effect of channel estimation error in the presence of Rayleigh fading [210]. Ohno provided analysis on the MMSE channel estimation error in OFDM systems and its impact on channel capacity in block Rayleigh fading [211]. Ohno used this work to propose optimal pilots to maximize capacity. While the capacity of these systems alone has been thoroughly analyzed, such analysis has not been combined with a ranging variance analysis to illuminate the trade-offs between capacity and ranging accuracy.

2.2.6 LEO PNT

Use of low-Earth orbit (LEO) constellations for positioning, navigation, and timing (PNT) dates back to the earliest operational satellite navigation constellation, TRANSIT [212]. Based on Doppler measurements extracted from narrowband UHF signals received from a single satellite at a time, TRANSIT required several minutes for convergence to a sub-100-meter solution.

The trade studies from which the Global Positioning System (GPS) was later conceived revealed that a medium Earth orbit (MEO) system with wideband signals would be more resistant to jamming than TRANSIT and would be capable of satellite-redundant instantaneous positioning with only a few dozen space vehicles (SVs) [212, Ch. 1]. L band was chosen because its wavelengths are short enough for ionospheric transparency, yet long enough to avoid significant attenuation due to rainfall and water vapor [213, 214, 54]. By now all traditional global navigation satellite systems (GNSS) have settled into a system architecture similar to that of GPS, to great success: billions of users across the globe benefit from low-cost, high-accuracy, near-instantaneous positioning and timing.

Nevertheless, the traditional GNSS architecture suffers from some deficiencies. Non-GNSS uses of the congested space-to-Earth spectrum in L band have prevented allocation of much greater bandwidth for GNSS in that band. Constellation survivability is limited by the small number of SVs, which make attractive targets for anti-satellite warfare [215, 216]. Jamming immunity is limited by the weakness of the signals, which, being diffused over an entire hemisphere, are easily overwhelmed [81, 76]. And positioning precision is limited by both signal weakness and bandwidth, which place information-theoretic lower bounds on ranging uncertainties [213].

In response to a pressing need for greater robustness and accuracy, GNSS has evolved over the past two decades. Several new constellations have been launched, and new signals have been introduced at separate frequencies—most with binary offset carrier waveforms that more efficiently allocate signal power [54, 212]. Nonetheless, GNSS remains principally MEO, L-band, and confined to a bandwidth occupying less than 125 MHz. Given tight budgets and enormous design inertia owing to the need for backward compatibility, radical changes in traditional GNSS over the next 30 years are unlikely. Spot beams, a promising feature of the GPS III program for improved jamming immunity [217], have been abandoned. Calls to introduce new GNSS signals in C band (e.g., [218]) have not gained traction. Upgraded SVs and more sophisticated receiver antennas will continue to extract gains in interference immunity, but likely not tens of decibels.

In short, traditional GNSS have been brilliantly successful, yet for some applications they remain inadequate with regard to accuracy, constellation survivability, or robustness to interference—for both civil and military users. To address these limitations, [9] introduces a concept for LEO PNT that exploits current and upcoming broadband LEO mega-constellations via a novel “fused” communications-and-PNT service. The practical costs and challenges facing past LEO GNSS proposals, including hosted-payload LEO GNSS and signal-of-opportunity (SoP) LEO GNSS, motivate the paper’s proposed architecture.

[9] makes three primary contributions. First, it summarizes the features of modern broadband LEO system design and operation relevant to dual-purposing such systems for PNT. Second, it presents a detailed concept of operations for *fused LEO GNSS*, to be defined in the next section. Third, it provides an analysis of the opportunity cost to constellation providers for re-allocating resources to provide a fused PNT service.

The earlier paper published in [219] is complementary to the present paper, which provides a complete description of the fused LEO GNSS concept and a detailed opportunity cost analysis. The reader is referred to [219] for analyses of achievable fused LEO GNSS positioning precision and anti-jam advantage compared to traditional GNSS. Summary values from these analyses are provided in Table tab:hostedvsfused for reference.

Expansion of GNSS back to the LEO ambit of TRANSIT beckons as a promising way to address the limitations of traditional GNSS. Mega-constellations of commercial satellites in LEO are being launched (SpaceX’s Starlink and OneWeb’s constellations) or planned (Amazon’s Kuiper constellation) to provide broadband connectivity across the globe. Such services’ global reach, low latency, and wide bandwidth situate them to revolutionize broadband communications.

[9] seeks to establish a less-obvious assertion: These constellations could also revolutionize satellite-based PNT. Their SVs are far nearer and more numerous than those of traditional GNSS in MEO or geostationary orbit, and their communications transponders have both exceedingly high gain and access to a vast allocation of spectrum. Potential commercial LEO PNT signals are thus more precise, powerful, and jam-resistant than those of traditional GNSS.

Dual-purposing LEO communications constellations for PNT is not a new concept. The emergence of the Globalstar and Iridium constellations in the late 1990s offered the prospect of LEO-provided navigation based on both Doppler and ranging. These constellations employ communications waveforms whose frequency and group delay can be measured opportunistically (i.e., without special cooperation by the constellation operator) and converted to typical GNSS observables: Doppler, phase, and pseudorange measurements [220, 221, 222, 223, 224, 225, 226] (see [212, Ch. 2] for definitions of these observables). But as with TRANSIT, only one or two Globalstar or Iridium SVs are simultaneously visible to a typical terrestrial user, preventing accurate instantaneous positioning. Instead, both theoretical [227] and experimental [222, 228, 229, 226] research has shown that several minutes of single-satellite passage across the sky are necessary for positioning to an accuracy below 100 meters. This remains true for IridiumNEXT, whose constellation is patterned after the original Iridium constellation [230].

The emergence of mega-constellations of LEO satellites whose signals can be exploited for many-in-view navigation, whether opportunistically or with the cooperation of the constellation operator, is an entirely new phenomenon. The literature exploring use of such constellations for PNT begins with [231, 232]. The current paper belongs in this category.

Although not originally intended for PNT, broadband mega-constellations are designed for rapid technological refresh via software or hardware, and so may be adaptable for PNT. But unlike traditional GNSS, in which costs are borne by nation-states and service is free-of-charge, commercial GNSS providers will seek to recoup costs from users. For such a scheme to be viable, it must be *economical*: that is, it must offer fundamental advantages over traditional (free) GNSS commensurate with the price tag, otherwise there will be no demand; and must be sufficiently inexpensive to provide, otherwise there will be no supply. [9] explores both facets of this problem.

In their groundbreaking work, Reid et al.[231, 232, 233, 234] analyzed the performance of potential LEO GNSS implemented using *hosted payloads*: dedicated PNT hardware onboard each satellite. There are good reasons to explore a hosted payload solution: Such payloads are modular, independent of the satellite's primary communications mission, and may be iterated and upgraded for future launches. As laid out by Reid et al., hosted PNT signals provide continuous global coverage and may be incorporated into user pseudorange navigation equipment nearly as readily as traditional GNSS signals. Reid et al. estimate that the system would enjoy a 30 dB improvement in signal-to-noise ratio, and thus resistance to jamming, over traditional GNSS.

A hosted payload approach along those lines is not radically dissimilar to traditional GNSS. No theoretical obstacle bars the way. However, space hardware development is costly and challenging as a practical matter. And a hosted payload would be costly: besides the cost of each payload, there are costs associated with renting space and hookups on the host satellite, costs for running necessary radiofrequency interference and compatibility testing, and both costs and risks of delay in securing the necessary frequency allocations.

A growing area of PNT practice draws measurements from so-called signals of opportunity (SoPs), typically wireless communications signals[235, 236, 225]. SoP techniques seek to eliminate the need for cooperation with the wireless system operator. Satellite downlink signals from the new LEO mega-constellations could be processed as SoPs, as has been done previously with the smaller Iridium and Globalstar constellations [222, 223, 224, 228, 229, 230, 226]. Such SoP-based LEO GNSS has several benefits. First, there is no need for cooperation with the constellation owner, which eliminates a potential coordination barrier to offering a PNT service. Second, users may exploit LEO SoPs without compensating the constellation owner, as has been the case with terrestrial cellular SoPs[225]. Third, since SoP-based PNT is necessarily passive, it preserves users' anonymity. Taken together, these three advantages are unique to SoP-based PNT and cannot be directly matched by non-opportunistic techniques.

Despite these advantages, SoP-based LEO GNSS suffers a key limitation, which might be termed the "few-in-view" problem. With fewer than four (or, in the case of Doppler-based PNT, eight) satellites in view, near-instantaneous cold-start PNT with inexpensive clocks is not possible: the time to achieve a PNT fix stretches from seconds, as with traditional GNSS, to several minutes, as with TRANSIT, Iridium, and Globalstar [237, 228, 238, 239].

One might expect LEO mega-constellations to provide greater SV coverage for SoP-based PNT than do the relatively small Iridium and Globalstar constellations. However, a large fraction of mega-constellation SVs will orbit at altitudes lower than Iridium and far lower than Globalstar, offering smaller terrestrial service areas per vehicle[240, 241]. Moreover, not all overhead satellites may direct energy to a given user's location. Although early SpaceX regulatory filings indicated its Starlink mega-constellation SVs would broadcast a quasi-omni-directional beacon signal to aid network entry, it is not clear whether such a beacon will always be present in the system as launched. Recent work by Neinavaie et al. detected Doppler-trackable beacons [242], but in a contemporaneous Starlink signal analysis the present paper's authors found that such narrow-band emissions appeared to be absent when the downlink was busy. Thus, beacon signals may only be sent when the downlink is idle, rendering them intermittent or totally unavailable once the system is more fully burdened.

Consequently, the only SoPs available from Starlink may be the broadband signals carried in narrow spot beams from each SV toward a small number of assigned compact service regions [243]. Significantly, the present authors' Starlink signal analysis has revealed that each service region is illuminated by broadband signals from at most two SVs. Thus, areas with no active subscribers may receive no broadband signals at all. Other broadband mega-constellation operators will likely adopt designs similar to Starlink's. The net effect, at any given instant, will be a reduction in the number of satellites actively illuminating the SoP user's location. [9] analyzes a scenario in which the global average number of SoPs from a LEO mega-constellation is less than that of Iridium by a factor of $6.3\times$. This takes single-mega-constellation-based SoP LEO GNSS from one-in-view to less-than-one-in-view, with a time to fix that will be unacceptably long for many applications.

Cooperation with mega-constellation operators could solve the few-in-view problem, enabling nearly-instantaneous-time-to-fix global PNT via traditional-GNSS-like multi-lateration. In this paradigm, PNT becomes a secondary service that augments the LEO mega-constellations' primary communications mission. Befitting its ancillary status, the PNT service ought not require significant changes to the SVs or to the constellation's allocation of on-orbit resources. [9] therefore focuses on solutions which "fuse" the requirements of PNT into the existing capabilities of the mega-constellation. In fused LEO GNSS, the hardware already designed and the spectrum already allocated for the satellites' primary broadband mission is dual-purposed for PNT. While this is also true of SoP LEO GNSS, fused LEO GNSS goes further to fully exploit the broadband signal's capabilities.

To support a fused LEO GNSS service, the constellation operator arranges for intermittent spot-beam coverage of areas where PNT users are present, providing signals from enough satellites for receivers to produce single-epoch stand-alone PNT solutions. Such cooperation also has the benefit of eliminating the duplication of effort associated with third-party tracking of orbits and clocks for a dense constellation.

Compared to hosted-payload LEO GNSS, fused LEO GNSS sacrifices nothing in performance while eliminating the costs of special-purpose on-orbit hardware. In fact, where previous proposals targeted positioning precision on par with traditional GNSS pseudoranging (on the order of $3\,$m), fused LEO GNSS can improve on this by more than an order of magnitude [219]. Moreover, it offers a significant anti-jam advantage over L-band hosted-payload solutions in terms of tolerable signal-to-interference ratio, thus making it attractive as a means for delivering assured PNT (A-PNT). This advantage comes at the cost of larger and potentially more expensive user equipment as compared to a hosted payload solution: for maximal anti-jam performance, a fused LEO receiver will require a phased array antenna. But for many applications, the user equipment, like the satellite hardware, will be dual-purposed for both communications and PNT: the same mass-market antenna and radio connecting a vehicle to a LEO communications network will be used for positioning at little additional cost.

These strengths emerge from two features of fused LEO GNSS. First, the plentiful data bandwidth present in each broadband satellite transmission burst permits supplying users with up-to-the-instant (and therefore highly accurate) orbit and clock products. Such orbit and clock products need not depend on atomic clocks onboard the SVs nor an extensive SV-observing network on the ground. Instead, the PNT service can employ a multi-tier GNSS architecture in which each SV's orbit and clock models are obtained via on-orbit precision orbit determination (POD) based on an onboard traditional GNSS receiver driven by a modest-quality clock [231]. Second, unlike traditional L-band services, commercial broadband signals in K-band and V-band have both high signal-to-noise-ratio (SNR) and large bandwidth. This greatly reduces receiver noise and multipath as a source of user ranging error, even when the ranging signal used over the communications link adopts the same structure and spectral profile as the usual communications signals. Furthermore, because these signals have a much shorter wavelength than traditional GNSS, it is possible to build a highly-directional receiver phased array for an additional $30\,$dB of anti-jam performance that is compact relative to its L-band equivalent.

PNT precision, anti-jam performance, and other constellation characteristics are compared in Table 3 for traditional GNSS, hosted-payload LEO GNSS, and fused LEO GNSS. SoP LEO GNSS is not included due to its few-in-view problem.

For use cases in which a hemispherical antenna is preferred, such as handheld devices, the fused SNR is not high enough to permit ephemeris and clock model updates via the

Characteristic	Traditional GNSS	Hosted[232]	Fused (hemi RX)	Fused (array RX)
Single-epoch PNT	✓	✓	✓	✓
Unlimited users	✓	✓	✓	✓
Low Earth Orbit		✓	✓	✓
Mega-constellation		✓	✓	✓
On-orbit POD		✓	✓	✓
Non-atomic clocks			✓	✓
Time multiplexed			✓	✓
Excess bandwidth			✓	✓
Zero age-of-ephemeris			†	✓
Highly directional				✓
Localized power boost	$$$	$	$	$
Precision horz.	3.0 m	3.0 m	37 cm	19 cm
Precision vert.	4.8 m	4.4 m	48 cm	25 cm
Anti-jam advantage	—	+30 dB	+25.3 dB	+56 dB
Maturity	Mature	Unproven		
Funding	Public	Private		
Cost to user	Gratis	Commercial		

Table 3: Contrasting traditional GNSS, previous hosted-payload proposals, and fused LEO GNSS. Precise orbit determination (POD) here assumes onboard GNSS receivers in LEO (multi-tier GNSS). Positioning precision is 95th percentile in the horizontal and vertical directions. Anti-jam advantage is compared to an L-band choke-ring antenna [219]. Because K-band downlink power is tailored to meet power flux regulations at ground level[244], variable atmospheric absorption due to e.g. weather is assumed to be compensated by increased transmit power at the SV.

† *If user downloads ephemeris via some other channel.*

standard broadband data link. Thus, a back-up communications link such as cellular data service would be required. Note that certain design elements that give fused LEO GNSS its performance advantage could be incorporated into future hosted payload proposals. However, [9] only makes comparisons against published proposals.

To be viable, a fused LEO GNSS service must be cost-effective for providers. As one of its key contributions, [9] shows that providing PNT service to every user in one service cell (e.g., for the Starlink constellation, a hexagon of up to 1090 km^2 [245]) is roughly as costly, in terms of constellation resources spent providing PNT signals, as a single 5.7 Msps downlink stream. Also, whereas broadband service expends constellation resources in proportion to the number and activity level of subscribers, GNSS service consumes resources in proportion to coverage area. For this reason, in dense urban centers where only a small fraction of potential broadband subscribers can be accommodated and alternatives for broadband connectivity abound, a fused LEO GNSS service could be a profitable complement to a mega-constellation's primary broadband mission.

Indeed, it has been observed [246] that effective subscriber density constraints in first-generation K_u broadband LEO systems could be severe. For this reason, population distribution statistics are invoked only indirectly in what follows, insofar as they are needed to predict the global distribution of downlink power expenditure onboard the SVs.

2.3 Spectrum Situational Awareness

Spectrum situational awareness (SSA) goes hand-in-hand with resilient PNT. Interference can present itself anywhere across the RF spectrum as attackers can target any subsystem of sensors on the HAV (e.g. GNSS receiver and FMCW radar). Identifying when and where a receiver is affected by interference is an important first step towards locating and mitigating the interference itself. Detecting and geolocating RF signals is a coveted capability as it facilitates search-and-rescue, tracking, and spectrum monitoring. LEO-based receivers are a proven asset for detecting, classifying, and geolocating terrestrial GNSS interference. Emitter geolocation from Low Earth Orbit (LEO) offers worldwide coverage with a frequent refresh rate, making it possible to maintain a common operating picture of terrestrial emitters, e.g. GNSS jammers and spoofers. Moreover, LEO satellites' stand-off distance from terrestrial interference sources permits tracking authentic GNSS signals, enabling precise time-tagged data captures from time-synchronized LEO-based receivers and precise orbit determination.

LEO provides a unique vantage point for observing GNSS interference: it is close enough to the source of the interference for a single sensor to characterize the strength, power spectra, and signal content of terrestrial jamming and spoofing sources, but far enough that authentic GNSS signals may still be tracked and navigation solutions computed. These observations permit geo-referenced characterization of terrestrial GNSS interference, which is an important step on the way to understanding the extent of the phenomenon and developing mitigation strategies. By working directly on 100 Hz data-wiped complex IQ correlation products instead of lower-frequency receiver products, it is possible to identify interference with greater sensitivity, permitting detection not long after it is first received [10]. Successive ground passes of the Fast, Orbital, TEC, Observables, and Navigation (FOTON) receiver aboard the International Space Station (ISS) form an impressively complete GNSS interference survey of the globe at latitudes below the ISS inclination of 51.6 degrees.

[11] explores single-satellite single-pass geolocation of terrestrial GNSS spoofing signals from Low Earth Orbit. GNSS spoofers transmit an ensemble of false GNSS signals intending that the victim(s) receiver will accept them as authentic signals and infer a false position fix and/or a clock offset. Receivers in LEO provide a unique opportunity to detect, classify, and geolocate terrestrial GNSS interference. Single-satellite-based transmitter geolocation is possible from Doppler measurements alone, assuming a carrier can be extracted from an interference signal. There are proven single-satellite Doppler-based geolocation algorithms, but they only apply to emitters transmitting at a constant frequency. By contrast, GNSS spoofers transmit signals whose carrier frequency contains an unknown time-

varying frequency component that imitates the Doppler corresponding to each individual spoofed navigation satellite. This paper develops a single-pass single-satellite technique that removes the unknown time-varying frequency component added by GNSS spoofers so that a Doppler (range-rate) time history can be extracted for geolocation. It is shown that the true range rate between the terrestrial spoofer and LEO-based receiver manifests in the spoofed receiver clock offset rate estimate. Monte Carlo simulations are developed that investigate how transmitter motion, transmitter clock offset rate, and spoofed clock offset rate affect geolocation accuracy. The proposed method is validated by simulating the reception of terrestrial GNSS spoofing signals on a LEO-based receiver and achieving under 10 km accuracy. Additionally, recent real-world GPS spoofing signals captured by a LEO-based receiver are analyzed. This section will present advances in interference localization from LEO as well as FMCW radar interference.

2.3.1 Interference Monitoring from LEO

GNSS signals are relied upon for a number of safety critical applications where there is a need for precise localization or clock synchronization. Due to the low strength of the signals at point-of-use, they are easily overwhelmed by RF interference — malicious or unintentional. This interference may simply deny a navigation and timing solution; it may also induce inauthentic solutions unbeknownst to the victim. Identifying when and where a GNSS receiver is affected by interference is an important first step towards locating and mitigating the interference itself. The work presented in [10] takes advantage of the receiver's rather unique platform — the International Space Station (ISS) — to detect GNSS interference as it is occurring. This task is aided by the fact that the ISS is one of the most-observed spacecraft presently in orbit; even if the navigation solution were severely degraded, a position estimate can be obtained from regularly updated public ephemerides.

The strength of a signal interfering with GNSS is also its Achilles' heel: it is easily heard, provided one is listening. A number of recent efforts have exploited this fact to monitor GNSS interference across the globe. One such approach takes advantage of the public Automatic Dependent Surveillance-Broadcast (ADS-B) used for air traffic control [247]. Interference was recognized as irregularities in ADS-B reports, which are collected by the community receiver network OpenSky. In fact, the authors of [247] were able to provide an estimate of the interference source's location by noting the effects on multiple flight paths and convex optimization techniques. This approach has its limits: the OpenSky Network's receivers are primarily (although not totally) located in populated areas with reliable internet access, with little coverage over oceans. Furthermore, the use of ADS-B means that it has limited coverage over conflict areas where overflights are rare but GNSS interference is likely to be present [248]. On the other hand, this approach is vindicated by the observation that GNSS interference tends to be inordinately powerful, affecting aviation up to 300 km from its estimated origin [249].

Commercial efforts have also entered the business of interference monitoring: hosted payloads managed by Aireon aboard Iridium NEXT satellites monitor ADS-B transmissions from orbit, enabling Aireon to observe areas not covered by OpenSky [250]. Yet another project takes advantage of data from over 500 reference receivers collected by organizations under the aegis of the International GNSS Service (IGS) [251]. It is desirable to search for GNSS interference in a way that is restricted to neither commercial flight paths nor the vicinity of reference stations. HawkEye360 is attempting to do exactly that: as a demonstration mission, three *Pathfinder* spacecraft launched in late 2018 were used to geolocate land-based reference signals [252, 253]. The Pathfinder spacecraft were placed in a Sun-synchronous orbit (SSO) at an altitude of 575 km, spaced apart by 100 to 200 km. Onboard software-defined receivers are capable of 144 MHz to 15 GHz; GNSS signals are well within this range in the L band (1 to 2 GHz). At the time of writing, HawkEye 360 has yet to publish its attempts to geolocate GNSS interference sources.

The signals are broadcast by high-power spoofing and jamming equipment that has the potential to disrupt GNSS-derived positioning, navigation, and timing (PNT) over a large geographic area. The strategies most effective at detecting and mitigating this interference depend on the (generally unknown) strategy used by the spoofer [78]. A simple, widely-implemented strategy requires the GNSS receiver to report when interference is present, prompting the user to discard the navigation solutions as invalid. This approach generally does not permit the user to entirely ignore the interference, as it can easily be strong enough to overwhelm the relatively weak GPS signal (at the Earth's surface). Being an eavesdropper in LEO, the FOTON receiver isn't itself led astray by spoofing attacks, although careful processing of raw captures can elicit the structure of the interference signal [254, §3].

There is also the possibility, not yet publicly demonstrated, that clever terrestrial interference could target an unsuspecting satellite in LEO. Such an attack could be particularly damaging to a satellite that relies on precise localization or timing for its mission, and not require a transmitter significantly stronger than those presently used to interfere with terrestrial receivers. Spacecraft-targeting interference would present an insurmountable challenge for the work presented here; one could then no longer make the assertion that the receiver is tracking authentic signals. However, spaceborne GNSS receivers in LEO are aided by the fact that any interference source on the Earth's surface will quickly fall out of sight as the spacecraft continues in its orbit.

Previous work in this area identified and located persistent sources of GNSS interference that were present over many ground passes [254, §4]. However, much GNSS interference is transient with a duration of only hours or days. Despite its shorter duration, transient interference can compromise the safety of GNSS-dependent systems, with implications for injury and economic damage.

Guided by NOTAMs, ADS-B data, and news reports, among other sources, it is possible to narrow down the search for transient GNSS interference [247]. [10]'s technical approach involves tuning the detection tests using these known sources of interference. Armed with a highly sensitive means to detect interference, it will be possible to identify heretofore unknown transient sources of GNSS interference over much of the globe from 2017 to the present. Additionally, this work has the advantage of a data set beyond compare: three years of 100 Hz data-wiped complex IQ correlation products captured by the Fast, Orbital, TEC, Observables, and Navigation (FOTON) receiver aboard the International Space Station (ISS).

There are two basic interference categories that this analysis can expect to find: narrowband and wideband. The latter may be due to spoofing or matched-code interference. Narrowband interference is the simplest and most common form of GNSS interference. It entails broadcasting a narrowband waveform in navigation bands for denial-of-service (DOS) purposes. On the other hand, a transmitter "spoofing" a GNSS signal broadcasts a counterfeit signal intended to deceive the recipient into thinking it is authentic. Somewhere in between these two techniques is matched-code interference, in which a GNSS satellite's pseudorandom ranging codes are broadcast sans navigation message; this is intended to fool receivers into acquiring the signal, but deny them a navigation solution. It is also possible that unintentional interference may be detected; for example, radio signals produced by malfunctioning electrical equipment or natural phenomena like solar radio bursts [81]. However, the former is less likely than intentional interference to be powerful enough to detect from LEO, and the latter is relatively rare. Nevertheless, it is important to rule out unintentional or natural interference to the extent possible before casting aspersions.

A simple technique by which GNSS interference can be detected is that of monitoring the carrier-to-noise ratio, C/N_0, also referred to as the carrier-to-interference-and-noise ratio (or CINR) in the presence of interference. GNSS interference manifests as a decrease in the C/N_0 of an authentic signal by a magnitude unlikely to be caused by multipath, the typical source of C/N_0 variation. Once a likely interference source has been detected, it may even be possible to narrow down its location on the globe by cross-referencing interference episodes with navigation solutions. The estimated carrier-to-noise ratio for each tracked signal is regularly reported by the receiver along with its navigation solutions, but this work has access to lower-level, higher-frequency, more sensitive receiver outputs: the complex IQ correlation products. Making the assumption that phase error remains negligible, the I (in-phase) component may be substituted for the C/N_0.

[10] extends existing methods for GNSS interference detection via C/N_0 monitoring from standard GNSS observables to higher-sampling-frequency complex correlation product data, and evaluates these methods on likely persistent instances of GNSS interference originating from hotspots identified in previous work.

The problem of identifying GNSS interference from data available to the receiver can be thought of as a special case of the more general anomaly detection problem; that is, determining whether or not observations of a stochastic process correspond to an expected (nominal) model, or an alternative (anomalous) model. Anomaly detection has been studied extensively [255, 256, 257]. More general approaches ([256, 257]) may be appropriate if the data domain is not amenable to analytical modeling. In the case of detecting GNSS interference from a receiver mounted on a spacecraft — especially one as well-studied as the ISS — it is possible for the model to incorporate patterns that may otherwise be classified as anomalies by a more domain-agnostic algorithm. One example of such features in the context of C/N_0 monitoring is the regular occultation of the GPS space vehicles (SVs) by the Earth. There are also features of the data that may be identified as anomalies, but are not of interest to this work. For example, rapid signal fading due to ionospheric scintillation [81, 258] is a natural phenomenon that is not as easily modeled. These features must be identified or ruled out in some other way.

A common limitation imposed on anomaly detection techniques is the restriction to a subset of the data, typically in the context of real-time detection [257]. As [10] studies historical data, the analyses herein are not constrained in this manner; however, the sheer quantity of data — years of 100 Hz data for each tracked signal — necessitates examining the data in segments.

There is strong interest in developing low-cost methods of detecting GNSS interference in order to (i) alert users that the navigation solutions may not be valid and (ii) if possible, recover the authentic solution. As (ii) is generally not a concern for the ISS, only methods to perform (i) are needed. A “low cost” solution is one that leverages quantities that are observable to a typical GNSS receiver installation, in comparison to those available only with specialized hardware [259]. Some common interference-detection metrics available to a typical GNSS receiver are:

1. Carrier-to-Noise (density) ratio, C/N_0 [260, 258, 81]
2. Received power (AGC gain) [260, 261, 258, 262, 81]
3. Spectral analysis [260, 81]
4. Number of observed signals [260]
5. Correlator output power [261]
6. Correlator output power variance [261]
7. Carrier phase vacillation [261]
8. Pseudorange outliers [263]
9. Signal quality monitoring (SQM) [258, 262]
10. Complex ambiguity function monitoring [264]

While the presence of an anomaly in one of these metrics can suggest interference, some successful detection strategies use more than one in order to improve the probability of detection or discriminate between different interference types [261, 258].

A problem related to anomaly detection is that of *quickest detection*, also referred to as quickest change detection (QCD) [265]. The goal of quickest detection is to identify a sudden statistical change in an observed signal with minimal detection delay. A key assumption made in quickest detection theory is that the duration of this change is effectively infinitely long — a change occurs only once in the signal's time history. More relevant to this work is transient change detection (TCD) theory, which studies to the case in which the change occurs only over an interval. A similar approach to the same underlying problem is termed *offline change point detection*[266]. Recently-published work in TCD has been adapted to fit this problem and forms the core of the statistical framework used to detect GNSS interference events.

GNSS such as GPS provide meter-accurate positioning while offering global accessibility, all-weather operation, and radio-silent reception. However, GNSS is fragile: its service is easily denied by jammers or deceived by spoofers. GNSS spoofers are becoming easily-accessible and low-cost, threatening GNSS-reliant systems [76, 145, 81]. Scientific satellites have received spoofing-like GPS interference over Ukraine and the Middle East [267, 268]. GNSS interference is not limited to military applications: the civilian maritime and airline industries have frequent encounters widespread GNSS jamming and spoofing. Corrupted Automatic Identification System (AIS) and Automatic Dependent Surveillance-Broadcast (ADS-B) messages from vehicles are frequently reported [247]. GNSS interference manifests as irregularities in AIS and ADS-B reports as these systems derive their position from GNSS. Ships near in Shanghai have fallen as victims to GNSS spoofing [151].

Fortunately, extensive progress in on-board GNSS spoofing detection and mitigation has recently been made [78]. Reliable spoofing detection techniques even exist for challenging environments such as dynamic platforms in urban areas where strong multipath and in-band noise are common [82, 79, 80, 65, 4]. Although reliable spoofing detection techniques exist, GNSS security can be further enhanced by accurately geolocating the source of interference.

Detecting and geolocating radio frequency (RF) signals is a coveted capability as it facilitates search-and-rescue, tracking, and spectrum monitoring. LEO-based receivers are a proven asset for detecting, classifying, and geolocating terrestrial GNSS interference [10]. Emitter geolocation from Low Earth Orbit (LEO) offers worldwide coverage with a frequent refresh rate, making it possible to maintain a common operating picture of terrestrial emitters, e.g. GNSS jammers and spoofers. Moreover, LEO satellites' stand-off distance from terrestrial interference sources permits tracking authentic GNSS signals, enabling precise time-tagged data captures from time-synchronized LEO-based receivers and precise orbit determination.

General stationary emitter localization with multiple receivers has been extensively studied [269, 270]. Time-synchronized receivers can exploit time- and frequency-difference of arrival (T/FDOA) to estimate the emitter location. In T/FDOA techniques, the differential Doppler and differential delay are first estimated, followed by the estimation of transmitter location. Another multi-satellite technique is direct geolocation, which is a single-step search over a geographical grid enabling estimation of the transmitter location directly from the observed signals [271]. Direct geolocation outperforms the two-step method in low signal-to-noise ratio (SNR) environments and short data segment scenarios.

Geolocation of moving emitters with multiple receivers using T/FDOA measurements is explored in [272, 273, 274, 275]. Geolocating moving transmitters becomes challenging as the transmitter's unknown velocity induces a Doppler shift. Rather than only estimating the position as in the stationary case, the velocity must also be estimated. Accurately geolocating a moving transmitter with a single receiver is impossible [276].

Several commercial enterprises such as Spire Global and Hawkeye360 have dedicated constellations for spectrum monitoring and interference geolocation efforts. These LEO constellations offer distributed time-synchronized LEO-based receivers whose data can provide accurate emitter geolocation. However, planning simultaneous multi-satellite captures to enable T/FDOA-based and direct geolocation can be difficult and expensive. [11] focuses on single-satellite platforms.

Single-satellite interference source geolocation accuracy is dependent on the transmitted waveform. Accurately locating emitters with arbitrary waveforms using a single LEO receiver is impossible in general: if the signal's carrier cannot be tracked, only coarse received-signal-strength (RSS) techniques can be applied for localization. However, if a carrier can be extracted, accurate single-satellite-based emitter geolocation is possible from Doppler measurements alone [277, 278].

The underlying technique of Doppler-based positioning was pioneered by research scientists at Johns Hopkins Applied Physics Laboratory, who solved the orbit of Sputnik-1 by analyzing the Doppler shift of the satellite's transmitted signal in 1957. Following this, the United States Navy deployed the first satellite-based geopositioning system (known as Transit) in 1960, which adopted this technique. The Transit satellites transmitted carrier frequencies at 150 and 400 MHz. Ground stations constantly looked for these transmissions and calculated the received Doppler. From Doppler curve(s), an initial estimated ground station position, and the transmitted orbit parameters, a least-squares estimator could produce a location estimate with errors as small as 100 meters [279]. In recent developments, a new global navigation concept is studied that relies on carrier Doppler shift measurements from a large LEO constellation [238].

A Doppler-based positioning technique much like that of Transit can be reversed for LEO-based emitter geolocation. If a LEO-based receiver can extract a Doppler history from an emitter, a geolocation estimate can be made. Doppler-based geolocation algorithms are effective because the range-rate between LEO-based receivers and terrestrial emitters varies rapidly over short captures. Performance bounds and error characterization for LEO-based single-satellite Doppler geolocation are presented in [280, 281].

Doppler-based emitter geolocation with a single LEO-based receiver was also proven by the University of Texas at Austin Radionavigation Lab (RNL). In collaboration with Cornell University, the RNL developed a software-defined multi-frequency GNSS receiver called FOTON that has been operating on the International Space Station (ISS) since 2017 [29]. Although emitter geolocation was not its original purpose, this single software-defined receiver has proven effective at locating emitters. Its data have been used to locate a powerful 70-watt matched-code jammer operating in Syria to better than 300 meters [254]. Localizing the emitter in Syria hinged on two lucky breaks: (1) the emitter was transmitting a GPS-like signal from which a Doppler history could be extracted, and (2) the emitter's signals had quasi-cosntant carrier frequency as transmitted. In addition to exploiting received Doppler, this work took into account transmitter clock rate errors to refine the geolocation estimate.

One of the key assumptions of the prior work is that the emitter transmits at a quasi-constant carrier frequency. The prior Doppler-based geolocation techniques falter if a transmitter introduces any significant level of complexity to carrier-phase behavior, such as frequency modulation or clock dithering. Assuming a nominally-constant transmitter carrier frequency is appropriate for GNSS matched-code jammers, but is fallacious for GNSS spoofers. GNSS spoofers do not transmit at a constant center frequency: they add an extra unknown time-varying frequency component to the spoofed signals that imitate the range-rate between spoofed GNSS satellite and the intend spoofed location. The extra unknown time-varying frequency component renders raw observed Doppler-based geolocation ineffective.

The range-rate between the LEO receiver and the terrestrial spoofer is common for each spoofed signal. If all of the spoofing signals are processed, a GNSS receiver's navigation solution estimator lumps any range-rate term that is common across all satellites into the receiver clock offset rate. Therefore, the time history of the receiver clock offset rate can be used for geolocation because it contains the range-rate between LEO receiver and terrestrial spoofer. Embedded in the range-rate time history is information about the transmitter's position.

[11] makes three primary contributions. First, [11] introduces a methodology to remove the unknown time-varying frequency component added by the GNSS spoofer, allowing the true range-rate between LEO-based spoofer and terrestrial spoofer to be extracted for geolocation. Second, the receiver clock rate offset time history can be corrupted by transmitter motion, transmitter clock rate error, and the spoofing induced receiver clock rate offset. Monte Carlo simulations are developed that investigate how these parameters affect geolocation accuracy. Additionally, the proposed method is validated by simulating the reception of a terrestrial GNSS spoofing signals on a LEO-based receiver. Lastly, recent real-world GPS spoofing signals captured by a LEO-based receiver are analyzed.

2.3.2 Radar Interference

Frequency-modulated-continuous-wave (FMCW) radars operate by transmitting a sequence of multiple linear chirps called a frame. After reflecting off of an object, the received signal is mixed with a replica of the transmitted chirp sequence, resulting in a beat frequency that indicates the range to the reflecting object. By examining the beat carrier phase shifts across multiple chirps, a radar can estimate the Doppler shift. Furthermore, an FMCW radar can estimate an object's direction through the phase shifts across elements in its antenna array. Since typical millimeter-wave (mmWave) FMCW radars use an intermediate frequency (IF) bandwidth in the 10s of MHz and a chirp slope in the 10s of MHz μs^{-1}, these radars sample a thin sliver of the time-frequency spectrum at any instant, making it unlikely that persistent interference will appear in the band of sensitivity and manifest as a false reflecting object [282, 283]. While this processing is generally effective for preventing false objects from non-adversarial interference, it leaves open an avenue for spoofed signals to be injected. By controlling the time-of-arrival and frequency offset of the spoofed signal, an attacker can force the target receiver to see fake objects at any arbitrary range and velocity. This type of attack could have drastic consequences for safe navigation on public roadways. An attacker capable of forcing a target vehicle to detect false objects could intentionally disrupt automated driver assistance systems (ADAS), causing unsafe maneuvering and collisions. Since FMCW radars are the most widely used radars in automotive vehicles [284], such spoofing capabilities could have widespread ramifications. Many studies have focused directly on the radar spoofing problem, demonstrating FMCW spoofing attacks with off-the-shelf devices [285, 286], custom spoofing boards [287], and spoofing on a realistic AV testbed [125]. The main limitation of this previous work is an assumption that the spoofer already knows the target radar's waveform, which is unlikely in a real-world scenario. Furthermore, the advanced spoofing attack in [125] was carried out using high-end test equipment, which is unlikely to be representative of actual radar spoofing threats. While not directly used for spoofing, Gardill et al. proposed a method of finding an unknown FMCW signal by analyzing the time-frequency spectrum of interference when mixed with a local fast-sweep rate FMCW signal [288]. Their study was then extended to demonstrate how such a tactic could be used to first estimate signal parameters, switch the local mixer to a CW signal to obtain precise timing, and then switch the local mixer to a time-aligned replica of the transmitted signal [289]. Such studies show that such a synchronization scheme is practical and that potential issues such as timing jitter can be accounted for. However, they do not propose a rigorous method of estimating chirp parameters, address parameter ambiguities, or analyze the optimality of mixing waveform selections. Additionally, they do not address the impact of estimation error, nor estimate Doppler shift, nor discuss tracking when the mixer is time-aligned. Other work has focused purely on synchronizing FMCW systems in time and frequency when the signal shape is known [290].

3 Vulnerabilities, Threats, and Mitigation for Local or Relative PNT Sensors

3.1 Roadside Sensing Technologies

A number of roadside sensing technologies are being considered or are in use for operations, planning, and safety assessment purposes. Some of these technologies are meant for temporary use; e.g. to collect data that can help in understanding future safety mitigation; and others are installed permanently; e.g. to assist in automated traffic operations. As explained in the next chapter, opportunities exist for these to augment the sensing technologies found on vehicles that can be a part of a cooperative system. This section introduces roadside technologies ancillary to direct PNT applications and identifies vulnerabilities that must be considered and mitigated for reliable performance.

3.1.1 Pedestrian Safety

In recent years, cities across the US have been promoting active transportation modes, such as walking and cycling, due to an abundance of environmental and economic benefits. However, according to data collected by the National Highway Traffic Safety Administration, a total of 6,516 pedestrians were killed in vehicular crashes in the U.S. in 2020. That reflects a 51% increase from fatalities over the last decade, while the share of walking trips has remained constant at 10.5%. Even accidents that do not involve fatalities carry an enormous societal cost, including property and motor vehicle damage, productivity losses, medical and administrative expenses, mental trauma, pain, and increased insurance premiums.

Some main causes of pedestrian crashes include distracted drivers, and failure to yield right of way. Multiple recent studies have also detected implicit racial yielding bias against pedestrians belonging to racial minority groups [291, 292]. As such, human error at multiple levels is a potential factor behind any pedestrian-vehicle collision. Consequently, unless we swiftly implement innovative strategies in the coming years, we can anticipate a significant escalation in both traffic congestion and safety issues. This concern is exacerbated by the projected 70 million population increase in the United States by 2045, with emerging urban megaregions expected to absorb 75 percent of this population growth, leading to a substantial rise in vehicle miles traveled.

In this context, enhanced levels of automation and communications within and between vehicles, but also out between vehicles and infrastructure, which we will refer to as connected and automated smart transportation systems (of which PNT services constitute a critical element, if not the most critical element), can contribute in important ways to improve mobility and enhance safety on US roadways, across the spectrum of road users and multiple modes. Specifically, PNT systems that utilize insight from roadside transportation infrastructure can allow for effective collision aversion. For example, a connected system can solve the “pedestrian around the corner” problem using roadside equipment (video imaging, infrared detection, or LiDAR) that detect the presence, speed, and trajectory of pedestrians (see Figure 4). In general, AI algorithms are applied to data gathered via cameras, radar, LiDAR, and the vehicle control system. AI methods include computer vision to interpret images and deep learning and neural networks to improve training algorithms and conduct virtual tests to improve the vehicle’s ability to respond.

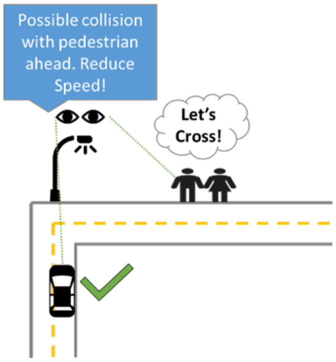


Figure 4: Illustration of the “pedestrian around the corner” problem

In considering the sensing of pedestrians, to this day, detection in the visible spectrum is still a challenging task due to appearance variations, illumination variations, occlusions, human motion variations, and background noise [293]. Thermal imaging also carries its own set of challenges, mostly around limitations in temperature variation. Scoring at best with accuracy rates of around 99% and varying dramatically among modes of transport being detected, no combination of technologies appears yet to be accurate or reliable enough for a sole determination in “life or death” PNT applications [294]. It is also possible to spoof a detection of objects. As explained later in sections on cooperative sensing, these need not discount the value of roadside technologies, as stronger resilience can be found when multiple technologies and applications are used together.

We conducted a comprehensive literature review on the state-of-the-art and the state-of-the-practice automated pedestrian data detection technologies. The outcome of this review is an assessment of the different automated data collection methods, including well-established and emerging AI- and sensor-based technologies, to evaluate their appropriateness and efficacy in different environments and for supporting data collection and usage efforts. Furthermore, we conducted a nationwide survey to identify best practices in the collection, analysis, and application of pedestrian-related data for safety and operational purposes. Additionally, we interviewed key stakeholders who have previously implemented these techniques to gain insights into their lessons learned and gather their expert qualitative opinions on the effectiveness of these technologies. In summarizing findings, our primary focus will be on Automated Video and LiDAR technologies, as these have emerged as the most promising solutions for PNT-related safety applications.

An online survey was sent to 194 experts within related agencies, institutions, and companies [294]. The purpose of the survey was to determine the extent to which different pedestrian count and detection technologies are being used, pedestrian technology attributes, use cases, and customer satisfaction levels. Out of the 194 recipients, 63 survey responses were submitted. Example of the responding agencies include Texas, Florida, Utah, Minnesota, and Massachusetts departments of transportation (DOT). The survey results are summarized below:

- **Technology Types:** 37% reported using passive infrared sensors, 21% used automated video technologies, and 18% used pressure or acoustic pads. However, the proportion of agencies using LiDAR and thermal imaging is significantly lower. Additionally, less than 5% of the agencies reported that they are implementing experimental programs for evaluating LiDAR and camera technologies.
- **Vendors:** The results show that Miovision products are the most commonly used for pedestrian counts. Regarding LiDAR technologies, only two respondents provided vendor names, Velodyne and BlueCity.
- **Automated Video Technology Advantages and Disadvantages:** Respondents reported several benefits, including a wide coverage area, the ability to use raw video files for safety assessment, high accuracy, vandalism resistance, ease of installation, no need to cut into the road, easy auditing, comprehensive coverage of pedestrian movement, and accurate volume and mode split data. It is also relatively affordable to procure and can be integrated with signal detection equipment. However, there are several disadvantages to consider. These include additional processing and subscription fees, high recurring costs, limitations in nighttime or windy conditions, susceptibility to weather-related challenges like fog and glare, potential algorithmic issues, and a requirement for AC power, usually at a signalized intersection.
- **LiDAR Technology Advantages and Disadvantages:** Advantages include the ability to gather new types of data, and high accuracy. On the downside, this method has not been thoroughly tested yet, and it entails a high cost for gathering, storing, and processing more refined or granular pedestrian information. Additionally, most applications do not require such granular data.
- **Thermal Imaging Technology Advantages and Disadvantages:** Respondents reported that this type of technology is more accurate than video technology in dark conditions and the presence of occlusion. However, they had concerns regarding lack of familiarity and testing, doubts related to accuracy and applicability for PNT.

3.1.2 Classical Detection Technologies

While this study focuses on infrastructure-based advanced pedestrian detection technologies, this section provides a brief explanation of traditional methods for pedestrian counting to give context to the discussion on emerging technologies and data sources. Classical techniques can be either manual or automated, with manual methods involving a required action (e.g. pushing a button) and automatic methods using sensors such as passive/active infrared, pressure mats, and radio beams.

Historically, agencies have relied on signal actuation buttons to communicate the presence of a pedestrian with drivers and traffic signals. Blanc et al. [295] conducted a pilot study to investigate the use of pedestrian signal actuation as a proxy for pedestrian volume. They found a linear relationship between pedestrian phase logs and the actual pedestrian volumes with an R^2 value of 0.70. While the analysis suggests that it is possible to make reasonable estimates of pedestrian volumes from this kind of pedestrian actuation, it depends upon site-specific adjustment factors.

In other cases, infrared sensors, which detect pedestrians by evaluating the difference between background thermal energy and heat emitted by people as they pass through the detection area, are used. TrailMaster, TRAFx, and EcoCounter are three commonly used infrared count device manufacturers. Pressure pads are another well-established technology. They detect pedestrians as they move over a pad using changes in weight. However, this type of technology is associated with many limitations. The Eco-Counter SLAB is the most used product in the market.

3.1.3 Emerging Sensing Technologies

The emerging sensing technology for Pedestrian Position Navigation and Timing (PNT) is a critical area of development that holds significant potential for improving pedestrian safety and navigation. This technology encompasses various innovations and approaches designed to enhance the accuracy, reliability, and versatility of pedestrian tracking and timing. Some key aspects and advancements in this field include:

- Computer Vision and Deep Learning
- Thermal Imaging Solutions
- LiDAR-Based Solutions
- Multi-Sensor Fusion

The upcoming sections will briefly discuss the history and main advancement in these technologies in the context of pedestrian detection and PNT. Also Tables 4 and 5 include an overview of the major finding related to the advantages and disadvantages of each technology, as well as the available vendors.

Computer Vision and Deep Learning
Computer vision, powered by deep learning algorithms, plays a pivotal role in pedestrian PNT. Advanced cameras and image processing techniques can identify and track pedestrians, even in complex urban settings.

In imaging-based technologies, one of the key tasks is to detect the presence of pedestrians in a video sequence or an image. In practice, this corresponds to recognizing the smallest rectangular bounding boxes that enclose the pedestrians [296] (see Figure 5). In order to automatically extract pedestrian information from video, objects must be detected, tracked from one frame to the next, and classified by type as pedestrians and non-pedestrians. (Note that different classifications may be needed for multi-modal or multi-purpose data collection). Deep learning methods are prominent techniques for achieving this task through the development of algorithms such as the You Only Look Once (YOLO) series and Faster-Region-based Convolutional Neural Network (Faster-RCNN) [297].

A typical computer visioning algorithm that detects pedestrians from traffic images involves the pipeline shown in Figure 6. The first step is collecting video streams. The next step is video preprocessing followed by object (i.e., pedestrian) detection which can either be conducted using traditional machine learning or deep learning algorithms.

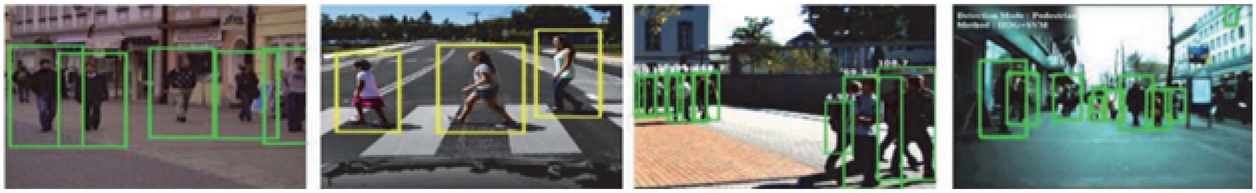
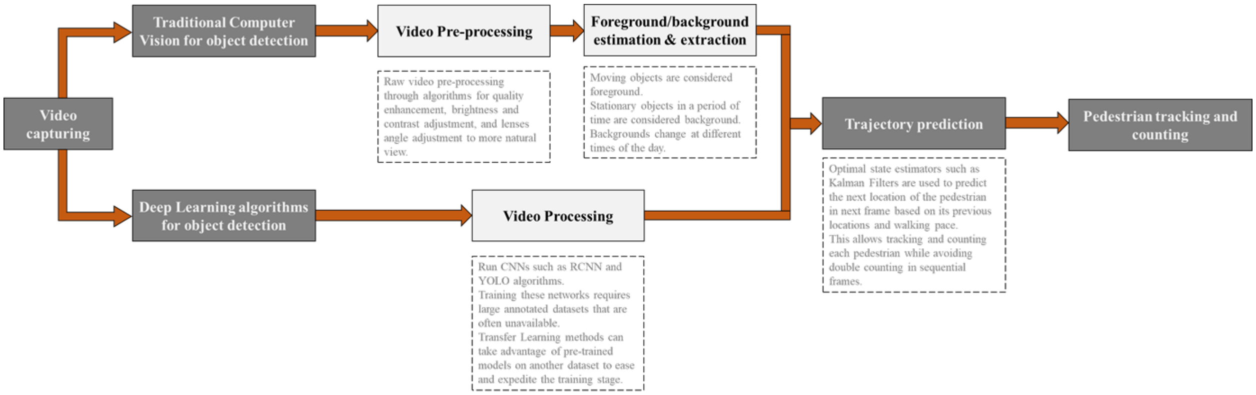


Figure 5: Example of pedestrian detection and tracking


Video capturing
Traditional Computer Vision for object detection
Video Pre-processing
Foreground/background estimation & extraction
Deep Learning algorithms for object detection
Video Processing
Trajectory prediction
Pedestrian tracking and counting

Raw video pre-processing through algorithms for quality enhancement, brightness and contrast adjustment, and lenses angle adjustment to more natural view.

Moving objects are considered foreground.
Stationary objects in a period of time are considered background.
Backgrounds change at different times of the day.

Run CNNs such as RCNN and YOLO algorithms.
Training these networks requires large annotated datasets that are often unavailable.
Transfer Learning methods can take advantage of pre-trained models on another dataset to ease and expedite the training stage.

Optimal state estimators such as Kalman Filters are used to predict the next location of the pedestrian in next frame based on its previous locations and walking pace.
This allows tracking and counting each pedestrian while avoiding double counting in sequential frames.

Figure 6: Computer visioning pipeline

Thermal Imaging Solutions

Thermal cameras are marketed as solutions for detecting pedestrians when the presence of visible spectrum is challenged, which include but are not limited to appearance variations, illumination and weather variations, occlusions, and human motion variations [293]. Unlike visual cameras, they operate like passive infrared sensors and generate infrared images by capturing the brightness intensity corresponding to the temperature and radiated heat of objects in the scene. Consequently, pedestrians that pass within the camera's field of view are detected by looking at heat signatures that are independent of illumination and appearance variations [298], [293]. Thermal image processing for pedestrian detection is composed of two steps: image capturing followed by automated image processing which in turn is subdivided into feature extraction and feature classification [299].

Both steps for thermal image pedestrian detection have shared characteristics with video-based detection technologies. Figure 7 shows the steps for capturing and processing thermal images for detecting pedestrians.

Thermal imaging technology is relatively new in the field of pedestrian counting, and its performance is still not fully known [300]. Only a few DOTs have reported their observations based on field experiments. Oregon DOT investigated thermal cameras for traffic signal detection purposes using FLIR's TrafiSense thermal traffic camera [301]. The undercounting rate was 49% (percentage of false negatives) while the percentage of overcounting was 5% (percentage of false positives). The results revealed that thermal cameras counted bicycles accurately in a controlled environment, but failed in real-life intersections. Florida DOT also performed field testing using FLIR TrafiOne thermal camera. For the field deployment at midblock crosswalk locations on two sites, the system resulted in an overall accuracy of 92%. The experiments showed that thermal cameras can detect pedestrians and slow-moving bicyclists, pedestrians on skateboards, and persons with disabilities, can be attached on the same pole as RRFBs and pedestrian crossing signs, can instantaneously trigger a traffic signal controller to request a pedestrian signal, similar to a push button, and can remove a call if the pedestrian walks out of the detection zone before the call is served.

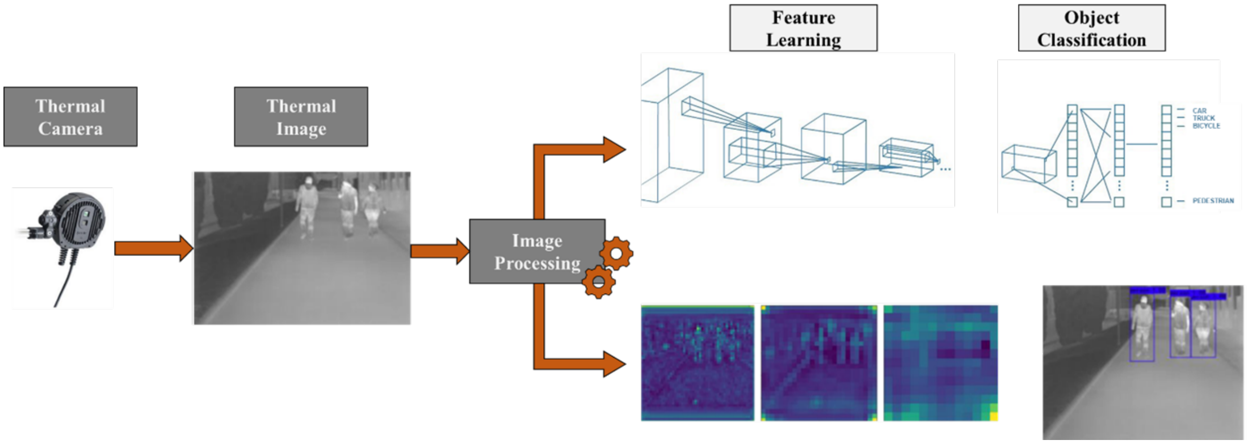


Figure 7: Conceptual framework for thermal pedestrian detection

LiDAR-Based Solutions

LiDAR sensors are increasingly being utilized for PNT applications. These sensors emit laser pulses to create precise 3D maps of the surrounding environment, allowing for accurate pedestrian detection and tracking. They are particularly effective in low-light conditions and adverse weather. Several research papers have explored the applicability of the LiDAR technology for pedestrian recognition and data collection (sometimes referred to as infrastructure-based detection systems versus vehicle-based detection systems). Compared to on-board LiDAR, roadside LiDAR sensors can cover a much wider detection range rather than just the environment vehicle. Additionally, roadside LiDAR has more advantages than onboard LiDAR because the latter require other supportive data sources, such as high-resolution 3D maps and GPS information. However, roadside LiDAR sensing systems are expected to work individually [302].

The LiDAR starts by emitting pulses of infrared light from the laser diode. A CPU records the time and direction of shooting. The pulse then travels and hits an object which in turn reflects a proportion of the infrared light where it is detected by a receiver. Then, the time and energy at which the infrared light is received are registered. Finally, AI algorithms pick up the raw data to create a complex 3D point cloud of the surface it is measuring based on its reflections and perform pedestrian detection and tracking. That is achieved through a set of steps which start with pre-processing the 3D point cloud by performing background filtering and object clustering then continues with pedestrian/vehicle classification and tracking [302]. Refer to Figure 8 for an example of a LiDAR 3D point cloud and processed clusters.

The 2019 study conducted by the Nevada Department of Transportation (DOT) represents one of the pioneering implementations of infrastructure-based LiDAR technology. Figure 9 shows the setup used for implementation. The detection and tracking rates of the proposed roadside LiDAR data processing procedure are all above 95%, and the valid detection range is about 30m (in one direction). The case study also investigated the use of LiDAR in bad weather conditions. Results showed that false rates increase from 0.14% in good weather to 1.01% in rainy weather and 1.87% in snowy weather.

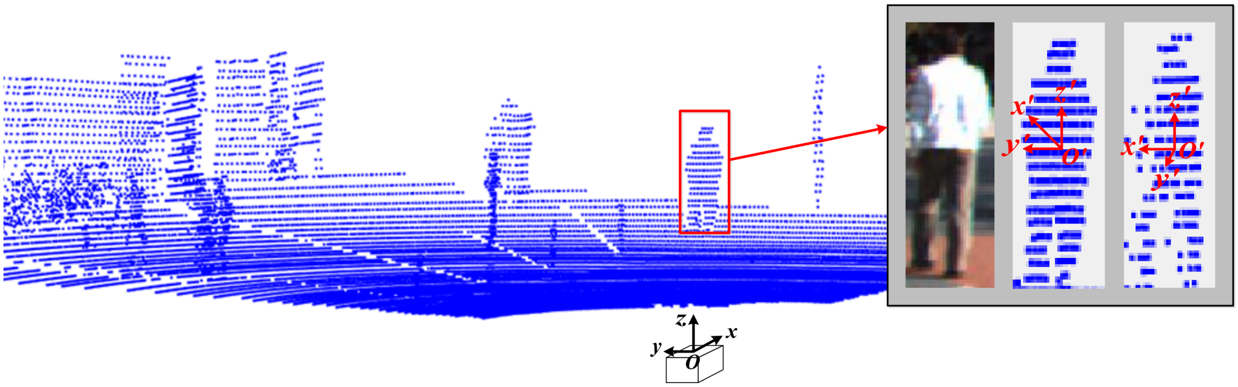


Figure 8: Example of pedestrian detection using a LiDAR generated 3D cloud [303]

Multi-Sensor Fusion

Combining data from various sensors, such as LiDAR, radar, cameras, and inertial sensors, enhances the accuracy and reliability of pedestrian PNT systems. This multi-sensor fusion approach provides a more comprehensive understanding of a pedestrian's (and all road users') position and movement. In practice, only products that combine thermal and RGB technologies are available. However, fusing data RGB, radar, and LiDAR is still in the research phase. Overall, the objective of these studies is to fuse feature-rich information from RGB images with sparse but reliable depth information from LiDAR point clouds or Radar data in order to improve the reliability of pedestrian detection systems. Some of the most recent advancements in this field can be found in [304, 305]. Figure 10 shows an example of a pedestrian detection setup that includes multiple sensors.

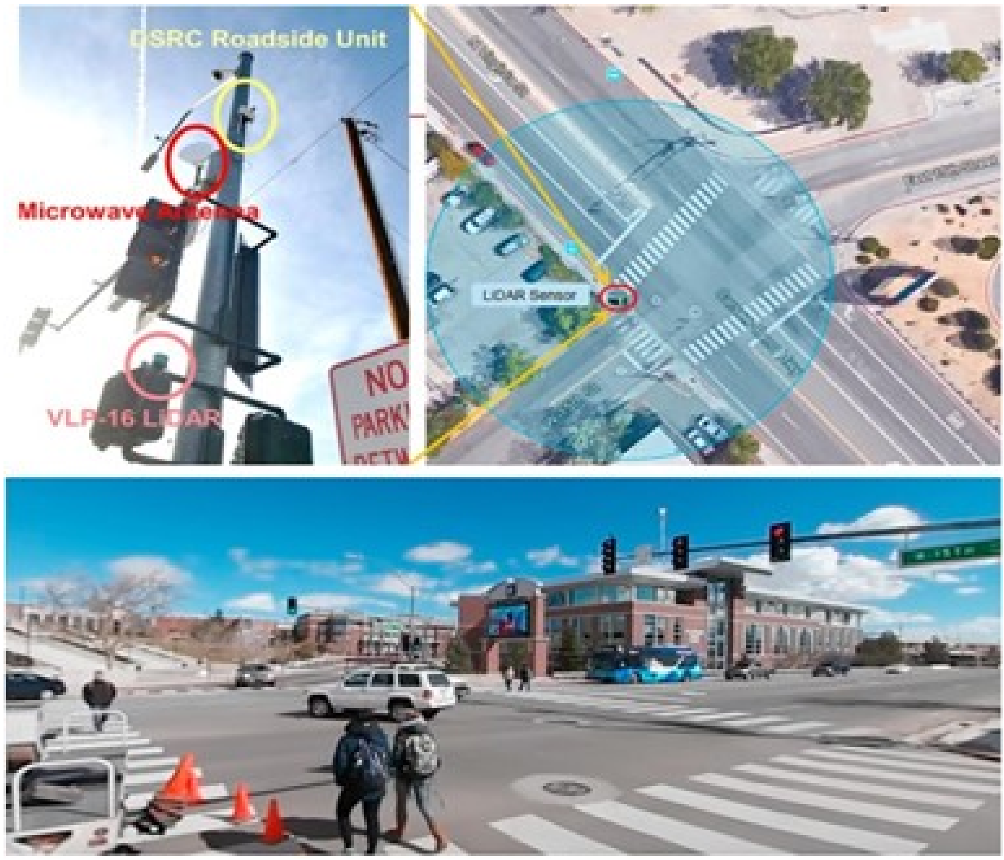
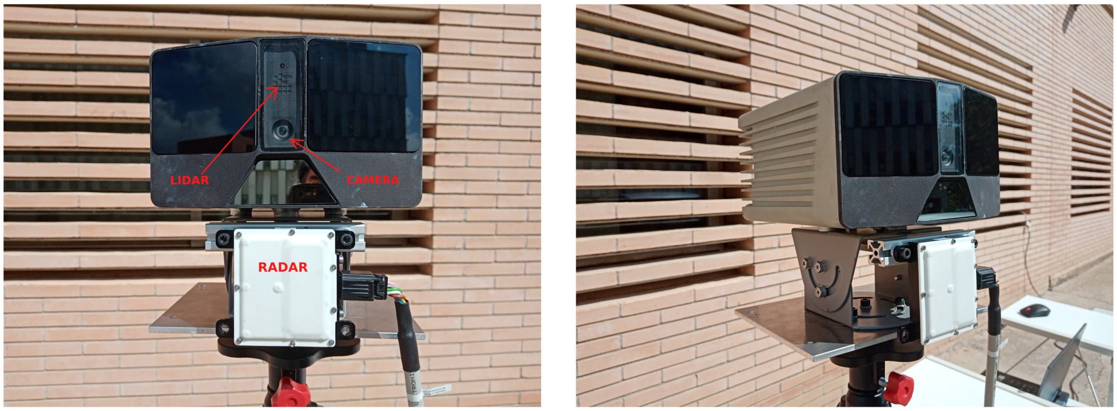


Figure 9: Infrastructure-based LiDAR implementation by Nevada DOT [302]



(a) (b)

Figure 10: Example of a setup for Multi-Sensor Fusion [305]

Table 4: Summary of findings at the technology type level [294]

Technology	Advantages/Benefits	Disadvantages/Challenges
LiDAR	• Reliable: works in different lighting and weather conditions • Overcomes occlusion • Overcomes lighting issues • Can capture multi-modal traffic data • Non-intrusive technology • 360º view • One LiDAR at the corner of the intersection is enough (which reduces installation and maintenance costs) • Can precisely measure the distance between objects; better suited for near-miss-detection application • Geolocates objects on a map • Simple installation requires ½ to 1 day • More accurate speed data • Can be used to ensure pedestrian safety on movable bridges • Best suited for real-time traffic control • Companies other than Velodyne have cheaper LiDAR sensors that are only 180º • More accurate than video detection • Large detection range • Tracks data without taking pictures • Can differentiate between axles, speeds, and shapes	• Has not been extensively tested yet • Agencies are reluctant to invest due to lack of experience with the technology and its accuracy • High cost of gathering, storing, and processing more refined/granular pedestrian information, which MPOs do not need • There aren't many vendors on the market • Velodyne has the only sensor in the market that has been tested for pedestrian detection and counting • Most agencies don't need 365/24 data • Lack of labeled data for training AI algorithms • Permanent LiDAR may cost over $20,000 • Tradeoff between height and blind spots • Not justified to be used for intersections • AV LiDAR algorithms don't work for roadside LiDAR • Sensor surface dirt can influence performance • Startups have a hard time of getting projects because transportation agencies are not very interested in using LiDAR • Counts large trucks as 2 vehicles • Blind spots with puck sensor • Cannot perform facial recognition • Does not capture license plates
Camera	• Best for multi-modal counts • Most vendors provide shelf-ready solutions • Video can be offloaded to a local third party for processing to save money • Can be used in challenging settings where infrared does not work, such as crowded locations and shared paths • Same technology can be used for detection and counting with a more complex algorithm • Video data can be used for many applications beyond pedestrian detection and counting • Edge computing overcomes storage issues • Edge computing overcomes security issues • Most vendors have clear security and privacy measures	• Expensive compared to traditional IR technology • Difficult to evaluate products and decide on a long-term procurement strategy • Agencies don't have large budgets to perform enough experimentation • Quality control standards are not established • Glare creates occlusions to data collection, even for the best cameras • Questionable accuracy in the dark and bad weather conditions • Shadows result in double-counting pedestrians • Accuracy definitions may be misleading: detection accuracy is different from count accuracy • When connecting to signal timing, multiple stakeholders need to be involved, and agencies need to get vendors on board • Significantly undercounts bikes in high-bike-volume locations • Different vendors use a different number of cameras • Micro-mobility adds noise and lowers performance • Edge computing does not allow accuracy checks • The system misses detection in the early morning and in dark/poorly lit conditions • Temporary products have battery limits and expensive hourly video processing fees • Security and political concerns • Existing infrastructure is low-tech and not suitable for smart devices • High recurring and maintenance costs • Permanent installation requires updating the communications network and infrastructure • Most vendors require purchasing new cameras • Video capabilities are not needed to count pedestrians on non-shared paths **Using CCTV and offloading to a third party:** • CCTV cameras do not have a proper field of view at intersections which deteriorates the accuracy and increases the need for off-the-shelf products
Thermal	• Mostly used for pedestrian detection • FLIR has several product offerings • More accurate detection than video technology in dark conditions and in the presence of occlusion	• Agencies are not familiar with this technology for smart traffic monitoring • Needs more testing • Limited detection range • Agencies need many sensors per approach • Does not distinguish between pedestrians and cyclists • Limited operating temperatures of the equipment
In-House Solutions	• Generally cheaper for system management and operation • Quarter the procurement price of off-the-shelf products • Most technologies are not very sophisticated and can be easily replicated in-house • Allow for more customization • If DOT owns the equipment, it can help small municipalities that can't afford consultants • Cheaper units allow spending more money on achieving a spatial distribution	• Require specialized personnel • Need to have a large active transportation program to develop, coordinate, and manage such as effort • Require more time and effort • Acquiring electronic components can be a big problem • Cloud-enabled communications are associated with service fees that add up quickly

Table 5: Summary of findings at the product/vendor levels [294]

Product	Accuracy	Cost	# Sensors or Cameras	View and Range	Power Source and Infrastructure Requirement	Data Transmission	Online Platform	Edge Processing	Live Feed	Night Vision	Traffic Controller Connection	Application and Output Types	Reputation and Reliability	Advantages	Disadvantages
Velodyne Puck Sensor + Blue City AI LiDAR technology Source: e-motec (2021)	• 98.7%	Procurement cost: • Puck sensor: $4,800 Recurring cost: • Unknown, depends on processing algorithms	1–2 / intersection	360º 100 m	• Pole • AC power source • IP addresses	100 Mbps Ethernet connection	✓	✓	✓	✓	✓	• Permanent • Intersection or midblock locations LiDAR sensor: • Cloud of surface points (x,y,z) • Distance between a data pt and sensor • Timestamp • 360º view Blue City AI: • Detection and classification of vehicles, cyclists, pedestrians • GIS trajectory data • Turning movement • Speed of road users • Near-miss detection • Red light violation • Jaywalkers • % of the time a crosswalk is used by pedestrians • Automated traffic signal performance matrix (ATSPM) • Wrong way detection	• Being piloted by CoA	LiDAR sensor: • Very large detection zone • Reliable in all light and weather conditions • High security and privacy • High accuracy • Low number of sensors required per intersection Blue City AI: • Provides surrogate safety analysis platforms to help city planners • Real-time access to signal performance metrics • Real-time access to safety metrics • Very large detection zone • Wide selection of outputs and metrics • AI-based algorithm	• Not widely used • Most agencies don't need 365/24 data
Velodyne Puck Sensor + LiDAR Matrix Inc. AI LiDAR technology Source: LiDAR Matrix ASWS Speed Study (n.d.)	• 99.5% detection accuracy • >98% traffic count accuracy	Recurring cost: • $1,000–1,500 for one day of data	1 / intersection	360º 90 m	• Traffic signal or light pole • AC power source (optional)	Manual	×	×	×	✓	×	• Temporary (battery life of 3–4 days) • Detection and classification of vehicles, cyclists, pedestrians • GIS trajectory data • Speed • Turning movement	• Developed for Nevada DOT and in use in ~50 locations. Implemented for smart RRFB in Las Vegas.	• LTE wireless connection for system status (battery life, data logging status, available storage space) • High accuracy • Wide range of outputs • Only one sensor is needed to cover an entire intersection • Comparable price to automated video technology	• Uses feature engineering instead of deep learning • Need to change batteries every few days • Sensor surface dirt can influence performance • A permanent arrangement would cost around $20,000
Miovision Scout camera Integrated video technology Source: Miovision Technologies (2021)	• >95%	Procurement cost: • $5,000 Recurring cost: • $10/hr video processing fee (can also use third-party algorithms)	2 / intersection	90°	• Sign or pole	Manual or 4G/LTE cellular	✓	×	×	×	×	• Temporary (72 hours) • Pedestrian, cyclist, vehicle, and e-scooter counts • Turning movement diagrams • Lane-by-lane volumes	• Trusted and frequently used product	• Portable • Can download video to be analyzed by a third party • Easy to install • Limited paperwork is needed. Can be installed without permission from multiple stakeholders • Miovision allows manual access to the data to avoid annual subscription fees	• Expensive video processing fees • Does not have real-time access • Limited battery life

Table 5: Summary of findings at the product/vendor levels (cnt'd.)

Product	Accuracy	Cost	# Sensors or Cameras	View and Range	Power Source and Infrastructure Requirement	Data Transmission	Online Platform	Edge Processing	Live Feed	Night Vision	Traffic Controller Connection	Application and Output Types	Reputation and Reliability	Advantages	Disadvantages
TrafficLink Integrated video technology Source: SmartCitiesWorld (2020)	• 99% count accuracy • 97% detection accuracy	Procurement cost: • $14,900 (includes hardware and software) Recurring cost (optional add-ons): • $500/yr signal communications • $750/yr continuous counts • $750/yr safety analytics	1 / intersection	360º 90 m	• Mounting height of 28–30 ft • Traffic pole • Mast arm • Signal post • AC power	Manual or 4G/LTE cellular	✓	✓	✓	×	✓	• Permanent • Designed for intersections • Stop bar detection • Vehicle, pedestrian, and cyclist count and turning movement count • Pedestrian delay • Occupancy ratio • Vehicle classification • Red light violation • Pedestrian compliance reports • Corridor travel time • ATSPM • Interactions with controller for advance detections	• City of Cambridge • CoA • Ohio DOT	• Only one camera is required per intersection • Can view crosswalks and stop bars on all approaches • Trafficlink web-based portal • Video and detection live stream through the portal • Provides signal phase status for operations • Provides alerts on operations status (power loss, low battery, telemetry unavailable) • Degraded video quality for privacy, storage, and streaming reasons • Local options for video storage that allow troubleshooting • Manually configurable detection zones • Base pricing includes 24/7 detection • If an agency has connectivity at the intersection (through video management systems (VMS)) it can stream in real-time (using RTS protocol) for no extra fee; otherwise, it needs to pay for the signal communications add-on (cellular device connection)	• Can only view the immediate intersection • Doesn't get to the upstream distance (450 ft dilemma zone operation) • Tradeoff between mounting height and coverage range. Needs to be mounted on a high location. • Need to set up communications independently or pay extra fees • Continuous counts are only available for an extra fee
Spack Solutions' countCAM3 Integrated video technology Source: Spack Solutions (2023)	Unknown	Procurement cost: • $1,300 • $300 external battery pack (optional) Recurring cost: • ~$300 for 24-hr video	1 / intersection	Unknown	• Sign or pole	Download data over Wi-Fi or hardwired connection	×	×	×	×	×	• Temporary (84 hours) • Intersection • Turning movement counts • Vehicular, pedestrian, and bicycle counts • Vehicular classification	• Tried by Delaware Valley Regional Planning Commission	• Cheap procurement cost • Agency can pre-schedule when the camera records video • 3-day turnaround service • Manual video counts • High accuracy	• Short battery life • Limited functionality
Eco-Counter CITIX – AI Integrated video technology Source: Eco-counter (2023)	95%	Procurement cost: • $10,900 • ~$2,500 for installation assistance (required) • $400 shipping Recurring cost: • ~$400/yr per unit	Unknown	20 m	• 5–7 m mounting height • Traffic pole • AC or DC power (does not come with a battery)	3G/4G connection	✓	✓	✓	✓	×	• Permanent • Designed for intersections • Pedestrian, cyclist, two-wheeler, and vehicle counts	• Clients are generally happy • A pilot study by NCDOT did not recommend it • Will be tested by TxDOT in the summer of 2022	• Self-contained (does not require access to signal) • Less expensive than Miovision • High-precision optical sensor (4K) • High precision for high-volume areas • Wireless data extraction • Has a wide-angle optical sensor that allows the sensor to cover several detection areas on the same site (several counting lines—user-configured) • Suitable for busy urban areas • Access to Eco-Visio online platform • Requires zero calibration	• Not widely used • Limited information available • Difficult installation (requires vendor installation assistance) • Functionality specific to counting

Table 5: Summary of findings at the product/vendor levels (cnt'd.)

Product	Accuracy	Cost	# Sensors or Cameras	View and Range	Power Source and Infrastructure Requirement	Data Transmission	Online Platform	Edge Processing	Live Feed	Night Vision	Traffic Controller Connection	Application and Output Types	Reputation and Reliability	Advantages	Disadvantages
Numina Integrated video technology	95%	Procurement cost: • ?? Recurring cost: • $1,500/yr per sensor	1 / approach for large intersections	90º 40 m	• Sign, pole, or building • AC power	Cellular LTE connectivity	✓	✓	×	×	×	• Permanent • Intersections or midblock • Pedestrian, cyclist, and vehicle counts • Location-based activity heatmaps • Speed (categorical) • Accuracy reports	• FDOT and Louisiana DOT pilots indicated low accuracy	• Edge processing, which guarantees privacy • Near-real time • Quarterly retraining of the algorithms • Hardware costs vary based on the number of sensors purchased. More sensors are discounted. • Involved in many pilots	• Rain can damage the units • Extreme weather affected reliability • Low accuracy, especially in crowded and shared paths • Recurring data subscription fees • Lose access to the sensor completely if recurring fees are not paid. The sensor itself does not have storage. • Cannot be used on fast highways and arterials. Cannot detect vehicles above 65 mph very well.
Street Simplified Integrated video technology	• 98% counting accuracy • 90% overall accuracy	Recurring cost: • ~$5,000 per intersection • Price is affected by the complexity of the location and the number of days	2 / intersection	Unknown	• Mounting location	Manual	✓	×	×	×	×	• Temporary (1–7 days) • Intersection or midblock • Counts cars (vehicle classifications), pedestrians, bikes • Vehicle trajectories • Near misses • Red light violation • Speeding • Jaywalkers • Pedestrian and cyclist compliance • Intersection blocking • Safety report	• Worked with the City of Houston and over 200 locations • Caltrans	• High-resolution video • Moving HQ to Austin soon • Can adapt the functioning to the environment • Does not require an external electricity source • Can't read license plates • Can't detect faces • Data is stored on the cloud • Client has full access to data on the cloud • Client can download video • Vendor is responsible for installing the equipment	• The client does not own the equipment • Results of pilot studies are not published yet • Company did not provide details about the equipment used
Boulder AI DNN Node Data processing solution Source: Boulder AI (2023)	Unknown	Unknown	1 / crosswalk	Depends on the camera	• Traffic pole • AC power	SD storage, connected to the internet over a cellular modem	✓	✓	✓	×	✓	• Permanent • Intersections • Multimodal continuous counts, including lane and turning movement analytics • Near-miss detection • Detects pedestrians and bikes at intersections and crosswalks • Speed detection • Red light violation • Turn infractions • Wrong way detection • License plate recognition, make/model • Advance and stop bar detection	• Not recommended by MAG and Massachusetts DOT	• One node supports up to 4 camera feeds • Works with inputs of CCTV cameras • Provides real-time data • Allows remote data management and service configurations • Can be used to implement automated touchless crosswalks, extend or recall crosswalk phase for safer crossings, or inform drivers via changeable or blank out signs	• 1080P resolution required for pedestrian detection • Does not distinguish bikes from pedestrians • Requires one camera per crosswalk • Overcounts by 79% • Counting accuracy is dictated by the lighting conditions, apparel of the pedestrian/bicyclist, and party size • Does not work very well with CCTV cameras due to their low resolution and improper view range
Boulder AI DNN Cam Camera-integrated solution Source: Boulder AI (2023)	Unknown	Unknown	1 / crosswalk	83º 90 m	• Traffic pole • AC power	SD storage, connected to the internet over a cellular modem	✓	✓	✓	×	✓	• Permanent • Intersections • Multimodal continuous counts, including lane and turning movements • Near-miss detection • Detect pedestrians & bikes at intersections and crosswalks • Speed detection • Red light violation • Turn infractions • Wrong way detection	• Not recommended by Massachusetts DOT	• 4k resolution camera • Provides real-time data • Allows remote data management and service configurations • Can be used to implement automated touchless crosswalks, extend or recall crosswalk phases for safer crossings, or inform drivers via roadside or blank out signs	• Does not distinguish bikes from pedestrians • Requires one camera per crosswalk

Table 5: Summary of findings at the product/vendor levels (cnt'd.)

Product	Accuracy	Cost	# Sensors or Cameras	View and Range	Power Source and Infrastructure Requirement	Data Transmission	Online Platform	Edge Processing	Live Feed	Night Vision	Traffic Controller Connection	Application and Output Types	Reputation and Reliability	Advantages	Disadvantages
												• License plate recognition, make/model • Advance and stop bar detection			
Currux Vision — Autonomous AI Systems Data processing solution	• 98% count accuracy • 97% detection accuracy • Speed with ±2 mph accuracy	Unknown	1 / approach	Depends on the camera	• Traffic pole • AC power	4G/Wi-Fi	✓	✓	✓	✓	✓	• Permanent • Turning movement counts at intersections along with colored dots for different classes of modes (vehicle, pedestrian, bike) • Vehicle classifications and speed studies • Trajectories • Speed • Wrong way detection and notification • Corridor travel time • ATSPM • Real-time near-miss notifications • Red light violation • Speeding • Crosswalk violation • Stop sign violation	• Used in San Jose • Recommended by MAG	• Capable of running a video from a CCTV camera • AI node can be connected to the internet over a cellular modem • Good accuracy • The system is flexible and can operate on highways, intersections, and city streets • Edge capability improves security • Based in Houston, TX	• Counting accuracy is dictated by the lighting position and party size • Missed detections are more likely in early morning and late evening • Requires one camera per crosswalk
Gridsmart Camera-integrated solution Source: Cubic (2022)	• 92% detection accuracy • 98% count accuracy	Procurement cost: • ~$18,000 Recurring cost: • $0	1 / intersection	180° 75 m	• Mast arm, off of a luminaire, or off of a strain pole	Data can be stored on the client's server, cloud, or USB	✓	✓	✓	×	✓	• Permanent • Intersections • Vehicle counts on roadway segments • Turning movement counts at intersections • Vehicle classifications • Interactions with controller for advance detections	• Not recommended by MAG	• Only one camera per intersection • Does not require any calibration, ever • Does not have to be aimed or focused • Easy to install • No recurring or licensing fees	• Only works with GRIDSMART cameras
Iteris Vantage Vector with Vantage Next Camera-integrated solution Source: Iteris (2020)	• 90% count accuracy • 98% detection accuracy	Procurement cost: • >$12,000 Recurring cost: • ??	1 / crosswalk	50° 120 m	Unknown	Unknown	✓	✓	✓	✓	✓	• Permanent • Intersections • Bi-directional pedestrian, bicycle, and vehicle counts • Pedestrian speed data • Detection alerts • Turning movement counts at intersections • Vehicle classifications • Corridor travel time • ATSPM with pedestrian delay and conflicts • Interactions with controller for advance detections	• Recommended by MAG and FDOT	• Includes video and radar technology • Very accurate • Large detection area • Iteris has multiple product offerings	• Expensive • Results of pilot studies are not available/published
TrafiOne – FLIR Thermal camera solution	• 99% detection accuracy	Procurement cost: • $6,000–8,000 per approach	2 / crosswalk	95° 15 m (8 detection zones can be defined)	• Traffic pole • AC power	• Cellular modem • Direct plug-in	✓	✓	✓	✓	✓	• Permanent • Intersections or midblock crosswalks • Tracks waiting and crossing pedestrians and bicyclists in urban environments	• Integrated with TAPCO's Wrong-Way Alert and	• Online platform for live video visualization and access data and review • Very high detection accuracy of 99% • Very accurate for vehicle counts • Flexible systems architecture	• Not very suitable for counting • Cannot distinguish pedestrians from bikes, but FLIR will be releasing a new module to do this in the future

Table 5: Summary of findings at the product/vendor levels (cnt'd.)

Product	Accuracy	Cost	# Sensors or Cameras	View and Range	Power Source and Infrastructure Requirement	Data Transmission	Online Platform	Edge Processing	Live Feed	Night Vision	Traffic Controller Connection	Application and Output Types	Reputation and Reliability	Advantages	Disadvantages
 Source: FLIR (2022)	• Not very suitable for counting	Recurring cost: • $35–50/ month for cellular service • ?? optional license for live feed				to the camera • Can be retrofitted with 5G cellular antennas to integrate with V2X						• Detects the presence of vehicles and bicyclists at the stop bar • Detects pedestrians and bicyclists in the crosswalk or on the curb • Turning movement counts • Wrong way detection and notification • Corridor travel time • ATSPM • Interactions with controller for advance detections	Pedestrian Crosswalk Systems • Used by FDOT		• Stop bar and advanced vehicle and bicycle presence detection require a separate, optional license • Need two thermal cameras to cover one crosswalk • System is susceptible to the presence of vehicles on crosswalks • Overcounts elements in the crosswalk • The system overcounts in higher magnitude in the early morning and daytime, compared to evening • Shading affects count accuracy
TrafiSense AI– FLIR Thermal camera solution Source: FLIR (2022)	Unknown	Unknown	Unknown	32° 30–90 m	• Traffic pole • AC power	• Cellular modem • Direct plug-in to the camera • Can be retrofitted with 5G cellular antennas to integrate with V2X	✓	✓	×	✓	✓	• Permanent • Detection by lane	• Integrated with TAPCO's Wrong-Way Alert and Pedestrian Crosswalk Systems • Used by FDOT • Sufficiently accurate based on field tests by Oregon DOT	• Similar to TrafiOne by FLIR	• Not able to distinguish between pedestrians and bicyclists • System is susceptible to the presence of vehicles on crosswalks • Only suitable for vehicle, bicycle, and pedestrian presence detection but not volume counts • Overcounts elements in the crosswalk • The system overcounts in higher magnitude in the early morning and daytime, compared to evening • Shading affects count accuracy • Video streaming is not available

3.2 Threats and Vulnerabilities in Vehicle-To-Everything (V2X) Communication Protocols and Applications

Various prior works have studied the security of Vehicle-To-Everything (V2X) technology. At the communication protocol layer, various prior works performed vulnerability analysis, but mostly on the protocol designs before the standardization of IEEE 1609 V2X protocol family [306, 307, 308, 309, 310]. On the latest V2X protocol family, Hu et al. performed the first formal security analysis and were able to uncover 4 new denial-of-service vulnerabilities in the Peer-to-Peer Certificate Distribution (P2PCD) design, which were all confirmed by the V2X protocol standardization group and the proposed solutions are planned to be integrated into future versions of IEEE 1609 [311].

At the application layer, various prior works have identified data spoofing as a realistic attack vector in the V2X environment (e.g., when malicious vehicle owners are malicious and deliberately send spoofed data). Specifically, various prior works have studied the impact of data spoofing attacks on V2V (Vehicle-to-Vehicle) based automated vehicle platoon systems and found that such spoofing attacks can cause collision or significant traffic flow instability [312, 313, 314]. Hu et al. are the first to design a formal security analysis method on such algorithms and were able to systematically discover 14 new vulnerabilities in popular platoon algorithm designs [311].

Besides V2V applications, prior works have also studied the impact of data spoofing attacks on V2I (Vehicle-to-Infrastructure) based intelligent transportation systems such as V2I-based intelligent traffic lights. Specifically, Chen et al. are the first to study such V2I-based systems, which are able to find that even data spoofing from one single attack vehicle can cause massive traffic jams due to a few newly-discovered security vulnerabilities at the traffic control algorithm level [315, 316]. Several follow-up works have performed more comprehensive security analysis [317] and designed potential defense solutions on both the infrastructure side [318] and vehicle side [319].

3.3 Threats and Vulnerabilities in PNT Systems, Sensors and Sources for HAT

We conducted an extensive literature review focusing on sensors and their sources applicable to Highly Automated Transportation Systems (HATSs). Our survey delves into the identification of subsystems and the specific sensors utilized within these subsystems. Furthermore, we extended our investigation to diverse scenarios, including urban and rural environments. The objective was to analyze the compatibility of each subsystem in both driving scenarios, highlighting the necessary sensors for optimal functionality.

The findings are summarized in Tables 6 and 7. The use of olive green shading in the cells signifies subsystems and sensors that are versatile and applicable in both urban and rural driving scenarios. In contrast, lime-colored cells indicate subsystems specifically suited

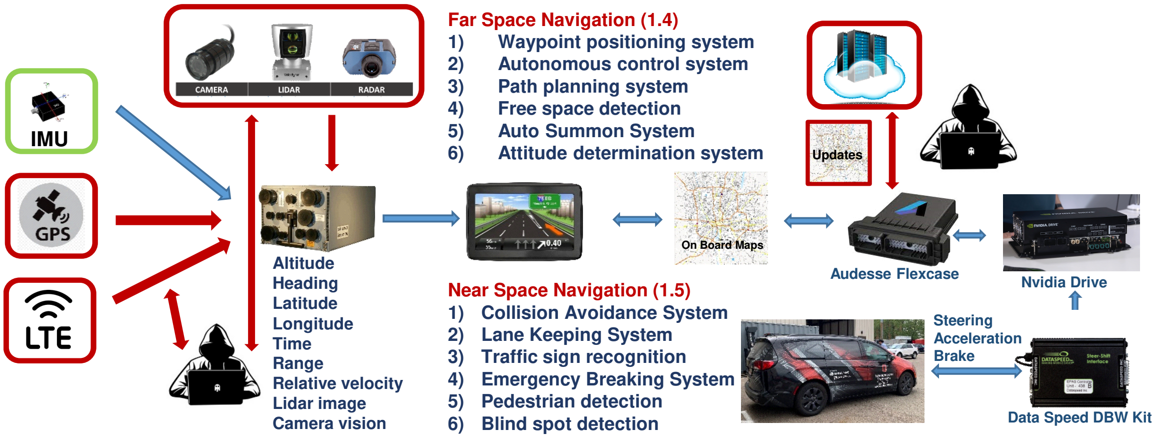


Figure 11: Framework for onboard subsystems and sensors for far-space and near space navigation

for developed urban areas, leveraging the availability of particular sources. Conversely, white cells denote instances where a given subsystem does not incorporate the associated sensor. The presence of a white cell in the tables also indicates a literature gap concerning the specific subsystem in relation to the sensors utilized in both urban and rural environments. This suggests that there is insufficient documented research or information addressing the vulnerabilities, threats, or impacts associated with the corresponding subsystem's sensors in diverse urban and rural settings.

These tables offer a comprehensive overview of the literature survey, presenting a detailed insight into the adaptability of subsystems and sensors across different driving scenarios within Highly Automated Transportation Systems.

We conducted an in-depth analysis of threats and vulnerabilities within both cellular and DSRC communication networks, considering all potential risks associated with WiFi and cellular communication networks. The outcomes of threats and vulnerabilities are comprehensively presented in Tables 8, 9, and 10. To specifically identify the implications for Positioning, Navigation, and Timing (PNT) subsystems, the system is categorized into two segments: near-space navigation and far-space navigation.

In near-space navigation, the PNT solution involves absolute positioning, necessitating decisions to be made within milliseconds. Conversely, far space navigation focuses on long-distance or strategic route planning, with decisions made over minutes. Figure 11 visually depicts the subsystems and their respective PNT solutions in both far-space and near-space navigation contexts. The tables and figures collectively provide a detailed examination of the threats and vulnerabilities associated with onboard navigation systems in various spatial and temporal contexts.

We conducted a comprehensive literature survey focusing on cooperative navigation strategies for connected autonomous vehicles operating within smart intersections. The existing body of literature revealed a limited number of papers specifically addressing cooperative navigation for connected autonomous vehicles. Notably, most of these papers primarily discussed Vehicle-to-Vehicle (V2V) cooperation, often restricting vehicle operations to straight roads in platoon formations. Some papers touched upon scenarios involving unsignalized intersections.

Recognizing the existing research gaps, we identified the need to develop a cooperative navigation strategy that leverages all available parameters from different sources, including Roadside Units (RSU), On-Board Units (OBU), Smart Traffic Lights (STL), and Autonomous Intersection Management (AIM) systems. Subsequently, we designed a cooperative navigation framework and proceeded to validate and verify several threat scenarios outlined in Tables 8, 9, and 10. This framework aims to address the limitations observed in the current literature and enhance the capabilities of cooperative navigation for connected autonomous vehicles at smart intersections.

Following the identification of sensors used in Highly Automated Transportation Systems (HATSs), we conducted an in-depth analysis of the attack surfaces associated with these sensors and sources for Positioning, Navigation, and Timing (PNT) solutions. Our investigation involved an extensive literature survey to identify potential threats and vulnerabilities of PNT sensors and sources. The results are systematically summarized in Tables 8, 9, and 10.

In Table 8, we present vulnerabilities linked to PNT sensors and sources that could be exploited by malicious actors to generate threats. Tables 9 and 10 outline the potential threats posed by attackers, leading to hazardous situations compromising the safety of road users. Within these tables, red cells indicate the types of threats or attacks that impact specific PNT sensors and sources, while white cells signify scenarios where a particular type of attack is not applicable to the corresponding sensors.

These tables provide a comprehensive summary of our literature survey, offering insights into the vulnerabilities, threats, and potential impacts on PNT sensors and sources within the context of Highly Automated Transportation Systems.

3.3.1 Waypoint Positioning System

The referenced literature provides an extensive overview of waypoint navigation systems employing diverse sensor technologies. Raja and Guven [320] focus on obstacle avoidance and waypoint navigation using global position and ultrasonic sensors. Sood et al. [321] explore multiple waypoint navigation in unknown indoor environments. Nofandi et al. [322] present the design of a floating robot for irrigation with GPS-based waypoint navigation. Lin et al. contribute to the field with research on local path planning and waypoint tracking using artificial potential fields for collision avoidance[323] [324]. Bao et al. [325] investigated the outdoor navigation of mobile robots through GPS waypoints and local pedestrian lanes. Stanczak et al. [326] enhance unmanned aerial vehicle communication in LTE-Advanced networks. Hussain et al. [327] propose an integrated approach of 4G LTE and DSRC for the Internet of vehicles. Miyake et al. [328] apply dynamic-task-based hazard identification to remote operation of experimental ships. Purucker et al. [329] specify system requirements for UAV-to-server communication. Storbacka [330] contributes to the development of autonomous navigation systems for maritime applications. Zhang et al. [331] propose a domain adversarial graph convolutional network for indoor localization. Naheem et al. [332] examine the tracking feasibility of UWB positioning systems for lighter-than-air indoor robot navigation. Mendes [333] explores drone-supported AI-based generation of 3D maps for indoor radio environments. Khassanov et al. [334] investigate finer-level sequential WiFi-based indoor localization. Dhanjal et al. [335] present Deeplocnet, a system for deep observation classification and ranging bias regression in radio positioning systems. Ma et al. [336] propose a WiFi RSSI ranking fingerprint positioning system for indoor activities of daily living recognition. Zhao et al. [337] develop a co-simulation platform for modeling and evaluating connected and automated vehicles and human behavior in mixed traffic. Naik et al. [338] focus on semantic mapping extension for OpenStreetMap applied to indoor robot navigation. Weerakoon et al. [339] introduce Terp, a reliable planning approach in uneven outdoor environments using deep reinforcement learning. Benders [340] explore reconfigurable path planning for fixed-wing unmanned aircraft using free-space roadmaps. The contributions in avionics navigation systems [341] and GIS-supported location-based services [342] further enrich the understanding of waypoint positioning systems.

3.3.2 Attitude determination system

The cited references delve into various methods and algorithms for attitude determination, primarily utilizing Global Positioning System (GPS) signals and sensors. Crassidis and Markley [343] introduce a new algorithm for attitude determination using GPS signals. Wang et al. [344] propose a constrained lambda method for GPS attitude determination. Liu et al. [345] present the Constrained Wrapped Least Squares method as a tool for high-accuracy GNSS attitude determination. Gan et al. [346] focus on real-time GNSS attitude determination with a direct approach, emphasizing efficiency and robustness. He et al. [347] survey the developments in attitude determination and control systems for microsats. Bar-Itzhack et al. [348] contribute algorithms for attitude determination using GPS. Wertz [349] and Markley [350] provide fundamental insights into spacecraft attitude determination and control. Gebre-Egziabher et al. [351] discuss the design of multi-sensor attitude determination systems. Lu [352] works on the development of a GPS multi-antenna system for attitude determination. Murrell [353] explores precision attitude determination for multimission spacecraft. Zhu et al. [354] propose a linear fusion algorithm for attitude determination using low-cost MEMS-based sensors. Collectively, these references offer a comprehensive exploration of sensor-based approaches to attitude determination in various contexts.

3.3.3 Path-Planning System

The surveyed literature, spanning references, collectively delves into various aspects of path planning systems, employing diverse sensors and methodologies. Zhang et al. [355]

propose an efficient algorithm for vehicle path planning based on taxi GPS big data. Maaref and Kassas [356] focus on optimal GPS integrity-constrained path planning for ground vehicles. Lee et al. [357] introduce an integrity-based strategy for urban autonomous vehicular navigation using GPS and cellular signals. Akhshirsh et al. [358] present a cost-effective GPS-aided autonomous guided vehicle. Corcoran [359] explores topological path planning in GPS trajectory data, while Wang et al. [360][360] investigate the impacts of GPS spoofing on unmanned surface ship path planning. Al Arabi et al. [361] discuss autonomous rover navigation using GPS-based path planning, and Korkmaz and Poyraz [362] propose path planning for rescue vehicles using segmented satellite disaster images and GPS road maps. Chung et al. [363] develop a path-planning algorithm for robotic lawnmowers using RTK-GPS localization. Li et al. [364] present an optimal path planning method for an autonomous underwater vehicle. Tan et al. [365] explore cooperative path planning for range-only localization using a single moving beacon. Imamura et al. [366] address outdoor waypoint navigation for an intelligent wheelchair using differential GPS and INS. Lekkas [367] explores guidance and path-planning systems for autonomous vehicles, while Crane III et al. [368] evaluate INS and GPS for autonomous navigation. Golenbiewski and Tewolde [369] propose a Wi-Fi-based indoor positioning and navigation system (IPS/INS). Ragothaman [370] investigates path planning for autonomous ground vehicles using GNSS and cellular LTE signal reliability maps and GIS 3-D maps. Ragothaman et al. [371] develop autonomous ground vehicle path planning in urban environments using GNSS and cellular signals reliability maps. Liu et al. [372] propose path planning for aerial sensor networks with connectivity constraints, and Ragothaman et al. [373] focus on autonomous ground vehicle path planning in urban environments using GNSS and cellular signals reliability maps: models and algorithms. Liu et al. [374] investigate remote driving over the LTE network. Challita et al. [375] utilize deep reinforcement learning for interference-aware path planning of cellular-connected UAVs, and De Bast et al. [376] discuss cellular coverage-aware path planning for UAVs. Mezghani and Mitton [377] address energy- and time-efficient dynamic drone path planning for post-disaster network servicing. Zhang and Zhang [378] propose a radio map-based 3D path planning for cellular-connected UAVs. Shin and Kim [379] present a PF-DOP hybrid path planning for the safe and efficient navigation of unmanned vehicle systems. Binol et al. [380] focus on time-optimal multi-UAV path planning for gathering data from roadside units. de Souza et al.[381] introduce real-time path planning to prevent traffic jams through an intelligent transportation system, and Shi et al.[382] address QoS-aware UAV coverage path planning in 5G mmWave networks. This collective body of work significantly contributes to the field by leveraging various sensors and methodologies, enhancing the capabilities of path-planning systems across diverse environments.

3.3.4 Collision Avoidance System

The literature review explores a comprehensive array of collision avoidance systems, drawing upon various sensors and methodologies. Almeida et al. [383] contribute insights into radar-based collision detection developments on the Unmanned Surface Vehicle (USV) Roaz II. Biswas et al. [384] emphasize reliability in vehicular collision avoidance through joint RFID and radar-based vehicle detection. Lazarowska [385] provides a review of collision avoidance and path planning methods for ships utilizing radar remote sensing. Sivakumar and Mangalam [386] delve into a radar-based vehicle collision avoidance system in four-wheeler automobile segments. Wang et al. propose an intelligent CAN-based automotive collision avoidance warning system.

Advancements in Vehicle-to-Vehicle (V2V) communication systems are explored by Wang et al. [387], presenting a novel V2V cooperative collision warning system utilizing UWB/DR for intelligent vehicles. Gazit [388] focuses on aircraft surveillance and collision avoidance using GPS. Toledo-Moreo and Zamora-Izquierdo [389] discuss collision avoidance support in roads with lateral and longitudinal maneuver prediction, fusing GPS/IMU and digital maps. Nieto and Dagdelen [390] develop a vehicle collision avoidance system based on GPS and wireless networks for open-pit mines. Rudel and Baldwin [391] investigate GPS relative accuracy for collision avoidance.

Several studies introduce innovative collision avoidance systems for diverse contexts. Ahamed et al. propose a train collision avoidance system using GPS and GSM modules. Young et al.[392] present a vehicle collision avoidance system using embedded hybrid intelligent prediction based on vision/GPS sensing. Sato et al. [393] contribute to vehicular collision avoidance support systems using GPS+INS hybrid vehicular positioning methods. Kose et al. [394] describe a collision avoidance expert system for an integrated navigation system. Elsayed et al. [395] present a fuzzy logic-based collision avoidance system for autonomous navigation vehicles.

The evolution of technology is evident in the integration of LTE-V2X communication systems for collision avoidance. Igual et al. [396] demonstrate and evaluate precise positioning for connected and automated mobility services. Alam et al. [397] focus on dynamic path loss exponent and distance estimation in a vehicular network using Doppler effect and received signal strength. Paier et al. [398] provide an overview of vehicle-to-vehicle radio channel measurements for collision avoidance applications. Viquerat et al. [399] discuss reactive collision avoidance for unmanned aerial vehicles using Doppler radar. Huang et al. [400] explore the use of the Doppler effect in an early warning system for a vehicle collision at a crossroads. Kihei et al. [401] leverage automotive Doppler sensing and machine learning in vehicle-to-vehicle networks for road safety. He et al. [402] enhance collision avoidance for distributed LTE vehicle-to-vehicle broadcast communications, while Li et al. [403] focus on a collision avoidance strategy supported by LTE-V-based vehicle automation and communication systems for car following.

LTE-V2X connectivity impact on global occupancy maps in a cooperative collision avoidance (CoCA) system is examined by Mouawad et al. [404], and the performance evaluation of safe avoidance time and safety message dissemination is investigated by Halim et al. [405].

Recent developments incorporate monocular vision, deep learning, and sonar fusion for enhanced collision avoidance. Rill and Faragó [406][409] utilize deep learning-based monocular vision for collision avoidance, and Hatch et al. [407] introduce obstacle avoidance using a monocular camera. Mahmeen et al. [408] propose collision avoidance route planning for autonomous medical devices using multiple depth cameras. Sawalmeh and Othman [409] provides an overview of collision avoidance approaches and network architecture for Unmanned Aerial Vehicles (UAVs). Tikar and Patil [410] propose a novel fast-responding driver assistance technique with efficient lane detection and collision avoidance using dynamic feature extraction in any environment. Jansen et al. [411] present real-time sonar fusion for layered navigation control. Wouter et al. [412] explore adaptive acoustic flow-based navigation with 3D sonar sensor fusion. The field of underwater autonomous vehicles is addressed by Kot [413], reviewing collision avoidance and path planning algorithms. Cao et al. [414] focus on obstacle detection and avoidance of autonomous underwater vehicles based on forward-looking sonar.

Lidar technology emerges as a pivotal sensor in collision avoidance systems. Fang et al. [415] propose a Lidar-driven spiking neural network for collision avoidance in autonomous driving. Kim et al. [416] investigate a numerical and experimental study on the obstacle collision avoidance system using a 2D Lidar sensor for an autonomous surface vehicle. Beul and Behnke [417] contribute to trajectory generation with fast Lidar-based 3D collision avoidance for agile Micro Aerial Vehicles (MAVs).

In conclusion, the surveyed literature reflects the dynamic landscape of collision avoidance systems, incorporating a diverse range of sensors and methodologies to enhance safety across various domains, including maritime, automotive, aviation, and underwater environments.

3.3.5 Lane Keeping and Departure System

The references in the literature provide an overview of various sensors and methodologies employed in the development and enhancement of lane-keeping and Departure Warning Systems in autonomous vehicles.

Enayati, Asef, and Jonnalagadda [418] introduce a novel triple radar arrangement for a Level 2 ADAS detection system in autonomous vehicles. Horri et al. [419] focus on mode-switching control using lane-keeping assist and waypoint tracking for autonomous driving in a city environment. Yang, Choi, and Chung [420] contribute to driving environment assessment and decision-making for cooperative lane change systems in autonomous vehicles.

Magosi et al. [421] conduct a survey on modeling automotive radar sensors for virtual testing and validation of automated driving. Kim et al. [422] propose lane change intention classification of surrounding vehicles utilizing open-set recognition. Feng et al. [423] verify a lane detection method with automotive radar based on a new type of road marking. Chetan et al. [424] provides an overview of recent progress in lane detection for autonomous driving.

Philipp, Schuldt, and Howar [425] focus on the functional decomposition of automated driving systems for the classification and evaluation of perceptual threats. Nagy and Costa [426] present the development of a lane-keeping steering control using a camera vanishing point strategy. Romano et al. [427] investigate the impact of lane-keeping assist system camera misalignment on driver behavior. Cantas and Guvenc [428] explore a camera-based automated lane-keeping application complemented by GPS localization-based path following. Basjaruddin, Rakhman, and Adinugraha [429] simulate the hardware of a lane-keeping assist system based on sensor fusion.

Lin et al. [430] propose an automatic lane marking detection method with low-density roadside LiDAR data. Pagire and Mate [431] discuss an autonomous vehicle using computer vision and LiDAR. Li et al. [432] contribute to road geometry perception without accurate positioning and lane information.

These studies collectively illustrate the diverse array of sensors and methodologies employed in the development of Lane Keeping and Departure Warning Systems, highlighting the multidisciplinary nature of research in this field.

3.3.6 Adaptive Front Lighting System

The references in the literature collectively provide insights into sensors and methodologies employed in the development of Adaptive Front Lighting Systems (AFS) and associated safety considerations in the context of driving.

Shadeed and Wallaschek [433] present the concept of an intelligent adaptive vehicle front-lighting assistance system. Kurtuluş [434] discusses exterior lighting systems for automated vehicles to communicate with pedestrians and other vehicles. Radoš et al. [435] focus on the modeling and implementation of an adaptive vehicle light management system. Dubal and Nanaware [436] delve into the design of adaptive headlights for automobiles, and Magar [437] explores adaptive front light systems for vehicle road safety.

Li and Zhao [438] contribute a low-cost and fast vehicle detection algorithm with a monocular camera for adaptive driving beam systems. Toney et al. [439] design and implement smart headlamps with overtaking assistance for automobiles using MATLAB. Rongier et al. [440] employ infrared thermography for the validation of thermal simulation of high-luminance LEDs used in automotive front lighting.

These studies collectively showcase the use of various sensors and methodologies, including intelligent algorithms, modeling, and infrared thermography, to enhance the capabilities of Adaptive Front Lighting Systems. Additionally, the focus on road safety underscores the importance of these technologies in improving driving conditions and preventing accidents.

3.3.7 Traffic Sign Recognition System

The references collectively address the advancements in Traffic Sign Recognition Systems (TSRS), emphasizing the integration of various sensors and methodologies to enhance driving safety. Zhao et al. [441] focus on obstacle avoidance for multi-sensor intelligent robots based on road sign detection. Yazdan and Varshosaz [442] contribute to the improvement of traffic sign recognition results in urban areas by addressing challenges related to scale and rotation. Le et al. [443] delve into the training of a Convolutional Neural Network (CNN) for transportation sign detection using synthetic datasets, exploring innovative approaches to optimize recognition capabilities. Hasan et al. [444] present a Traffic Sign Recognition System employing Support Vector Machines (SVM) and CNN, emphasizing the crucial role of such systems in promoting driving safety through efficient sign recognition.

3.3.8 Night Vision System

Presented references address the development of intelligent systems for enhanced safety in driving conditions, particularly focusing on Night Vision Systems. Dhelia et al. [445] present ”Protall,” an Intelligent, Multi-sensor, Comprehensive Obstacle Avoidance System designed for both automobiles and Unmanned Aerial Vehicles (UAVs). This system incorporates various sensors to provide a comprehensive solution for obstacle avoidance. On the other hand, Kamble and Patil [446] introduce an Intelligent Night Vision System for automobiles based on computer vision, emphasizing the role of advanced imaging technologies in enhancing visibility during low-light conditions. Additionally, Priyadharshini et al. [447] contribute to the field by proposing a Surveillance-based approach for spotting and categorizing automobiles, highlighting the relevance of such systems for monitoring and ensuring safety in driving scenarios, particularly at night.

3.3.9 Emergency Braking System

The referenced papers collectively delve into the intricate domain of Emergency Braking Systems (EBS) within the realm of autonomous vehicles, offering comprehensive insights into various facets of these systems. EBS assumes a pivotal role in ensuring vehicular safety, employing a sophisticated blend of multi-sensor fusion, advanced algorithms, and communication technologies. The integration of diverse sensors such as radar, GPS, lidar, and cameras is extensively explored in references [454], [455],[456], and [457], highlighting the pursuit of optimizing emergency braking algorithms through the synergy of multiple sensing modalities.

Understanding the influence of advanced emergency braking systems in critical scenarios is a focal point, as evidenced by the investigation presented in reference [458]. This research emphasizes the significance of evaluating how these systems perform in high-

Table 6: Subsystem Verses Sensors and Sources in Urban-Rural Driving Scenarios

HATS-PNT Sub-system	***Radar***	***GPS***	***INS***	***Doppl***	***LTE***	***Camei***	***Sonar***	***Lidar***	***WiFi***	***Legacy Maps***
Waypoint Positioning		[320][321] [322][324] [323][325]			[326][327] [328][329] [330]				[331][3 [333][3 [335][3	[337][338] [339][340] [341][342]
Attitude Determination		[343][3 [345][3 [347][3	[349][350] [351][352] [353][354]							
Path Planning		[355][3 [357][3 [359][3 [361][3 [363]	[364][365] [366][367] [368][369]		[370][357] [371][372] [373][374] [375][376] [377][378] [379]				[380][3 [382][3	[378][380] [381][382]
Collision Avoidance	[383][3 [385][3 [387][4	[388][3 [390][3 [449][3	[393][3 [395][3	[397][3 [399][4 [401]	[402][3 [449][4 [450][4 [405]	[406][4 [408][4 [331][4	[411][4 [413][4 [451]	[415][452] [416][417]		
Lane Keeping	[418][419] [420][421]			[422][423] [424][425]		[426][427] [428][429]		[430][453] [431][432]		
Lane Departure	[418][419] [420][421]			[422][423] [424][425]		[426][427] [428][429]		[430][453] [431][432]		
Adaptive front lighting	[433][434] [435][436]					[437][438] [439][440]				
Traffic Sign Recognition						[441][442] [443][444]				
Night Vision						[445][446] [447]				

stakes situations, shedding light on their behavior to minimize the severity of potential collisions. The importance of simulation, testing, and real-world validation is underscored by references [459], [460], [461], [462], and [463], collectively emphasizing the need for a rigorous approach to assessing the effectiveness and reliability of emergency braking systems across diverse scenarios.

Furthermore, references [464] and [465] explore the integration of the Internet of Things (IoT) and data analysis to enhance emergency braking systems. Real-time data analysis is positioned as a key component, facilitating continuous monitoring and enhancing the system's responsiveness to potential dangers. Concurrently, research in references [466], [467], and [468] focuses on object detection, tracking, and front-view camera-based systems to fortify the capabilities of emergency braking systems. The accurate identification and tracking of objects in the vehicle's path are highlighted as crucial elements for enabling timely and reliable emergency braking responses, thereby elevating overall safety.

Additionally, the development of low-cost autonomous emergency braking systems for electric cars is explored in references [469], [463], and [470]. The pursuit of cost-effective solutions holds the promise of democratizing access to advanced safety features, potentially amplifying road safety on a broader scale. In essence, the amalgamation of these research endeavors contributes to the continuous evolution of Emergency Braking Systems, aligning with the overarching goal of advancing safety measures within the autonomous vehicle landscape.

3.3.10 Pedestrian Detection System

The references provide valuable insights into the realm of Pedestrian Detection Systems, exploring a diverse array of sensors and methodologies to enhance safety in driving scenarios.

Reference [471] examines the interplay between automated vehicles and pedestrian safety, delving into the potential and limitations of pedestrian detection. The paper emphasizes the importance of understanding the promises and challenges associated with deploying such systems.

In reference [472], the focus shifts to millimeter-wave radar-based pedestrian trajectory tracking for autonomous urban driving. The utilization of radar technology showcases the potential for precise pedestrian tracking, a crucial aspect for ensuring the safety of both pedestrians and autonomous vehicles.

A novel approach to non-line-of-sight pedestrian detection is presented in reference [473], where secondary radar employing frequency doubling is explored. This innovative technique aims to enhance the detection capabilities, particularly in scenarios where direct line-of-sight visibility is compromised.

Reference [474] introduces a model-based pedestrian tracking system utilizing automotive radar. The paper outlines a novel approach to pedestrian tracking, showcasing the integration of radar technology for improved accuracy in detecting and monitoring pedestrian movements.

The concept of generalizable multi-camera 3D pedestrian detection is explored in reference [475]. Leveraging multiple cameras, this approach aims to provide a comprehensive and adaptable system for detecting pedestrians in varied environments.

The integration of thermal cameras for pedestrian detection is discussed in reference [476]. Thermal imaging adds a new dimension to pedestrian detection systems, enabling the identification of pedestrians based on their thermal signatures, particularly useful in low-light or challenging visibility conditions.

Event-based pedestrian detection using dynamic vision sensors is presented in reference [477]. This methodology leverages dynamic vision sensors to capture relevant events, offering a real-time and efficient approach to pedestrian detection.

Nighttime pedestrian detection and distance estimation are addressed in reference [478], introducing a Multi-task Faster R-CNN. This method is designed to improve detection performance during low-light conditions, contributing to enhanced safety in nighttime driving scenarios.

Lidar-based pedestrian detection is the focus of reference [479], providing an overview of the application of lidar technology in advanced driving assistance systems. The paper discusses the benefits and challenges associated with lidar-based pedestrian detection.

Finally, reference [480] explores the detection and tracking of pedestrians using Doppler lidar. This methodology capitalizes on Doppler lidar technology to enhance the precision of pedestrian detection and tracking, particularly in dynamic environments.

In summary, these references collectively contribute to the advancement of Pedestrian Detection Systems, showcasing a diverse range of sensor technologies and methodologies aimed at enhancing safety in driving scenarios by effectively identifying and tracking pedestrians.

3.3.11 Blind Spot Detection System

The referenced papers collectively provide insights into Blind Spot Detection systems, showcasing various sensors and methodologies employed to enhance safety in driving scenarios.

Reference [481] focuses on a multi-sensor fusion algorithm within a cooperative Vehicle-Infrastructure System for Blind Spot Warning. By integrating data from multiple sensors, the algorithm aims to enhance the accuracy of blind spot warnings, contributing to improved driving safety.

In reference, [482], a micro-Doppler radar is utilized for Pedestrian Detection in blind areas, coupled with motion classification based on rush-out risk. This approach leverages radar technology to detect pedestrians in areas typically considered blind spots, enhancing overall awareness for drivers.

The technical challenges and a proposed solution related to blind spots in autonomous cars are discussed in reference [483]. The paper addresses the complexities associated with blind spots in autonomous vehicles, emphasizing the need for effective solutions to ensure safety during autonomous driving.

Reference [484] investigates driver glance behavior towards cyclists at intersections, specifically in the context of being caught in the blind spot of a truck. The study employs a choice model to analyze driver behavior, providing valuable insights into potential blind spot issues and associated safety concerns.

In reference [485], a path planning method is proposed for wheeled mobile robots, considering blind spots. The approach utilizes the Robot Operating System (ROS) navigation stack and a dynamic window approach to enhance path planning, emphasizing the importance of accounting for blind spots in the navigation process.

In [486], the authors present a Blind-Spot Monitoring System using LiDAR. LiDAR, a remote sensing technology, is employed to detect and monitor blind spots around a vehicle. The system aims to enhance driver awareness by providing real-time information about objects in the vehicle's blind spots, ultimately contributing to safer driving. Reference [487] focuses on an experimental study evaluating the capabilities of long-range LiDAR in sensing safety distances for vehicle applications. The study explores the potential of LiDAR to accurately perceive safety distances, crucial for effective blind spot detection. By experimenting with long-range LiDAR, the research aims to contribute to the development of advanced safety systems, particularly in the context of blind spot monitoring. Both [486] and [487] underscore the significance of LiDAR technology in addressing blind spots, leveraging its capabilities for precise and reliable detection. The use of LiDAR in blind spot detection systems enhances safety by providing drivers with comprehensive information about their vehicle's surroundings, minimizing the risk of collisions, and improving overall driving awareness.

Overall, the references highlight the significance of addressing blind spots in driving scenarios and propose diverse sensor technologies and algorithms to enhance detection and awareness, ultimately contributing to increased safety on the road.

3.3.12 Parking Assist System

The literature collectively provides a comprehensive overview of Parking Assist systems, detailing the diverse sensors and methodologies employed in this context, along with considerations for associated safety in driving scenarios.

[488] focuses on the system design of automatic parking assist based on ISO26262 standards. ISO26262 compliance ensures that the automated parking system adheres to safety standards, highlighting the commitment to designing and implementing reliable and secure parking assistance features.

[489] delves into the subjective evaluation of intelligent parking assist systems, emphasizing the importance of considering typical parking scenarios. This research contributes to enhancing the user experience and safety aspects of parking assistance technology.

[490] presents an algorithm for human classification in automotive radar systems. This classification algorithm is pivotal for ensuring that the parking assist system accurately detects and responds to human presence in parking spaces, preventing potential accidents.

[491] introduces a SqueezeNet-based approach for range, angle, and Doppler estimation in automotive MIMO radar systems. This method enhances the precision of radar systems, crucial for the accurate functioning of parking assist features [492] explores automated parking tests using Inverse Synthetic Aperture Radar (ISAR) images from automotive radar. The utilization of ISAR images contributes to the evaluation and improvement of radar-based parking assistance systems.

[493] introduces imaging radar for automated driving functions, emphasizing the role of radar technology in providing visual information crucial for safe and efficient parking assistance. [494] proposes an intelligent parking lot assistance system based on machine vision and the A* algorithm. This fusion of machine vision and algorithmic intelligence contributes to precise and effective parking assistance.

[495] offers a survey of smart parking application deployment, shedding light on the various technologies and approaches applied in the deployment of smart parking systems. [496] and [497] explore the development of parking assistance systems and the establishment of safety metrics for automatic vehicle parking using machine learning, respectively.

[498] discusses a smart parking system mobile application using ultrasonic detectors, showcasing the integration of mobile applications with sensor technologies for convenient and safe parking. [499] presents a solution for autonomous vehicle parking, contributing to the advancement of self-parking technologies.

[500] and [501] [524] focus on Lidar technology for parking assistance and self-driving cars, respectively, underlining the significance of Lidar in enhancing perception and safety in parking scenarios.

[502]concludes the collection by discussing car parking assistance based on time-of-flight cameras, adding to the diverse sensor technologies employed in parking assist systems and their contributions to safety in driving scenarios.

3.3.13 Parking Space Detection System

The references provide comprehensive insights into Parking Space Detection systems, highlighting various sensors and methodologies employed to enhance parking efficiency and contribute to driving safety.

In reference [503], Convolutional Neural Networks (CNNs) are explored for parking space detection in downfire urban radar. The use of CNNs demonstrates their effectiveness in radar-based systems for accurately identifying vacant parking spaces. Reference [504] investigates the fusion of radar and camera technologies for vacant parking space detection. The integration of these two sensor modalities aims to improve the reliability and precision of parking space detection systems.

A research review on parking space detection methods is presented in reference [505], offering an overview of diverse approaches and methodologies employed in this domain. The paper provides valuable insights into state-of-the-art techniques in parking space detection.

In reference [506], a millimeter-wave dual-lens antenna is proposed for an IoT-based smart parking radar system. This innovative antenna design contributes to the development of radar systems with improved capabilities for detecting parking spaces.

The utilization of automotive millimeter-wave Synthetic Aperture Radar (SAR) for an auxiliary parking method is explored in reference [507]. This approach leverages SAR to enhance parking assistance systems, showcasing the potential of radar technologies in parking applications.

A connected car-based parking location service system is introduced in reference [508]. The system utilizes connected vehicles to provide real-time information about available parking spaces, contributing to efficient parking management.

LTE signal-based vehicle localization in indoor parking lots using mobile phones is discussed in reference [509]. The paper presents a novel approach to parking space detection by leveraging LTE signals and mobile phone data.

Reference [510] introduces a connected vehicle-based parking space guidance system, leveraging advancements in connected vehicle technologies to offer guidance and information about available parking spaces.

Underground parking lot navigation using Long-Term Evolution (LTE) signals is explored in reference [511]. The use of LTE signals enhances navigation systems, providing accurate information about parking spaces in indoor environments.

An edge-based smart parking solution using camera networks and deep learning is presented in reference [512]. The combination of cameras and deep learning algorithms contributes to real-time parking space detection and management.

Drone-based vacant parking space detection is discussed in reference [513]. Drones are employed as a novel tool for monitoring and identifying available parking spaces, offering a dynamic and flexible approach to parking space detection.

In reference [514], Convolutional Neural Networks (CNNs) are applied to on-street parking space detection in urban networks. The use of CNNs showcases their effectiveness in visual-based parking space detection systems.

Real-time IP camera parking occupancy detection using deep learning is explored in reference [515]. Deep learning algorithms applied to IP camera feeds enable accurate and real-time detection of parking space occupancy.

An image-based approach for parking spot detection with occlusion handling is presented in reference [516]. The proposed approach addresses challenges related to occluded parking spaces, contributing to more robust parking space detection.

On-street parking spot detection for smart cities is discussed in reference [517], focusing on the development of systems that enhance urban parking management and contribute to the efficiency of smart cities.

Mapping and semantic modeling of underground parking lots using a backpack lidar system is explored in reference [518]. Lidar technology is employed for 3D mapping of parking spaces, contributing to advanced parking infrastructure.

Parking space detection based on camera and lidar sensor fusion is investigated in reference [519]. The fusion of camera and lidar data enhances the accuracy and reliability of parking space detection systems.

In reference [520], a parking line-based Simultaneous Localization and Mapping (SLAM) approach is proposed using Advanced Driver Assistance Systems (ADAS) sensors. This approach leverages sensor fusion for rapid and accurate loop closing and parking space detection.

A smart parking system using WiFi and wireless sensor networks is introduced in reference [521] [523]. The integration of WiFi and wireless sensor networks contributes to the development of smart parking solutions with enhanced communication capabilities.

In reference [522], an IParking system is presented as a real-time parking space monitoring and guiding system. The system utilizes advanced technologies for real-time monitoring and guidance in parking facilities.

A real-time parking space monitoring and guiding system, named iParking, is presented in reference [523]. The system utilizes advanced technologies for real-time monitoring and guidance in parking facilities, contributing to efficient parking management.

In conclusion, the references collectively illustrate the diverse range of sensors and methodologies employed in Parking Space Detection systems. These technologies aim to improve parking efficiency, reduce congestion, and enhance overall driving safety by providing real-time information about available parking spaces.

3.3.14 Valet Parking System

Literature collectively provides insights into the development, methodologies, and safety considerations associated with Automated Valet Parking (AVP) systems, highlighting the various sensors and techniques used in these systems.

[524] focuses on time-optimal nonlinear Model Predictive Control (MPC) for radar-based automated parking. MPC is crucial for optimizing vehicle trajectories during the parking process, contributing to efficiency and safety. [525] introduces RVDet, a feature-level fusion of radar and camera for object detection. This fusion enhances object detection capabilities, ensuring the accurate perception of the vehicle's surroundings during parking maneuvers. [526] discusses the development, analysis, and real-life benchmarking of exploring random Trees (RRT)-based path planning algorithms for automated valet parking. Path planning algorithms are vital for determining safe and efficient routes during parking.

[527] presents a robust multi-camera Simultaneous Localization and Mapping (SLAM) approach with Manhattan constraint, contributing to precise mapping and localization crucial for automated valet parking. [528] provides a survey on the evolution from smart parking to autonomous valet parking, addressing challenges and future directions. This review outlines the advancements and considerations in the transition to fully automated valet parking. [529] describes a fully automated valet parking system based on infrastructure sensing, emphasizing the role of sensing technologies in achieving fully autonomous parking.

[530] introduces an autonomous valet parking system with Asynchronous Advantage Actor-Critic Proximal Policy Optimization, showcasing advancements in reinforcement learning for parking automation. [531] explores the design, user experience, and business opportunities associated with automated valet parking using IoT. This research provides a holistic view of the design and user perception of AVP systems. [532] discusses radar-based multi-floor localization for automated valet parking, addressing the challenges of multi-level parking environments.

[533] focuses on visual place recognition for automated valet parking, leveraging semantic and geometric descriptors to enhance the precision of localization. [534] introduces AVP-LOC, a surround-view localization and relocalization system based on an HD vector map for automated valet parking. This approach emphasizes the importance of high-definition mapping for precise and reliable parking.

In summary, these references collectively contribute to the understanding of the sensors and methodologies employed in automated valet parking systems, with a strong emphasis on enhancing safety, efficiency, and user experience.

3.3.15 Auto Summon System

Literature collectively provides insights into the intelligent and connected aspects of vehicles, emphasizing current scenarios, future directions, and challenges, with a specific focus on cybersecurity, automotive software, and smart summoning of vehicles.

[535] discusses the current situation, future directions, and challenges of intelligent and connected vehicles. It provides an overview of the state of the technology, potential future developments, and the challenges that need to be addressed for widespread adoption. [536] focuses on cybersecurity attacks in vehicular sensors, highlighting the vulnerabilities associated with connected vehicles. It emphasizes the importance of securing vehicular sensor systems to ensure the safety and reliability of connected vehicles.

[537] presents a review of automotive software in connected and autonomous electric vehicles. It provides insights into the role of software in enabling connectivity and autonomy in vehicles, addressing key aspects of the evolving automotive landscape. [538] introduces the concept of smart summoning of ambulances during a vehicle accident. This innovative approach leverages connectivity and intelligent systems to enhance emergency response by autonomously summoning an ambulance to the accident location. [539] discusses integrated perception and tactical behaviors in an auto-organizing aerial sensor network. While not explicitly focused on auto summoning, it highlights the integration of perception and tactical behaviors in connected sensor networks, showcasing the broader applications of intelligent systems in the automotive domain.

In summary, these references collectively contribute to the understanding of intelligent and connected vehicles, covering topics such as the current state of technology, cybersecurity challenges, automotive software, and innovative applications like smart summoning for emergency response.

3.3.16 Adaptive Cruise Control System

Literature collectively provides insights into Adaptive Cruise Control (ACC) systems, covering various aspects such as multianticipation, environmental challenges, brake performance, fault-tolerant control, congestion mitigation, real-time distributed control, radar technology, and the development trend of ACC for ecological driving. Here's a summary:

[540] introduces multi-anticipation for string-stable adaptive cruise control, proposing a method to increase motorway capacity without relying on vehicle-to-vehicle communication. [541] discusses the impact of mud-snow layer accumulation on ACC system radar and proposes a method for measuring the thickness of the accumulated layer. [542] analyzes the brake performance of radar-based adaptive cruise control during ramp merging using simulation software.

[543] presents a robust non-fragile fault-tolerant control approach for ensuring the safety of cooperative adaptive cruise control systems. [544] focuses on congestion-mitigating

model predictive control design for adaptive cruise control based on Newell's car-following model. [545] proposes a real-time distributed cooperative adaptive cruise control model considering time delays and actuator lag.

[546] discusses MIMO FMCW radar with Doppler-insensitive polyphase codes, contributing to radar technology for ACC. [547] enhances velocity estimation based on joint Doppler frequency and range rate measurements. [548] reviews the development trend of adaptive cruise control for ecological driving, providing insights into the evolution of ACC systems. [549] explores the automatic recognition of sonar targets using feature selection in micro-Doppler signature, showcasing advancements in sensing technologies relevant to ACC.

In summary, these references collectively contribute to the understanding of ACC systems, addressing various challenges and proposing innovative solutions for improving their performance and safety.

Table 7: Subsystem Verses Sensors and Sources in Urban-Rural Driving Scenarios

HATS-PNT Subsystem	***Radar***	***GPS***	***INS***	***Doppl***	***LTE***	***Camer***	***Sonar***	***Lidar***	***WiFi***	***Legacy Maps***
Emerg Braking	[454] [458] [455] [456] [457]	[459] [464] [465] [550]	[466] [460]	[551] [461]		[462] [467]	[468] [469]	[463] [470]		
Pedes Detection	[471] [472] [473] [474]					[475] [476] [477]		[478] [479] [480]		
Blind Spot Detection	[481] [482] [483]					[481] [484] [485]		[481] [486] [487]		
Parkin Assist	[488] [489] [490]			[491] [492] [493]		[489] [494] [495]	[496] [497] [498] [499]	[500] [501] [502]		
Parkin Space Detection	[503] [504] [505] [506] [507]				[508] [466] [509] [510] [511]	[504] [512] [513] [514] [515] [516] [517]		[518] [512] [519] [520]	[521] [522] [523]	
Valet Parking	[524] [525] [526] [527]	[528]				[527] [529] [530] [531]		[532] [533] [534]		
Auto Summon	[535] [536] [537]	[538]				[539] [537]		[536]		
Adapti Cruise Control	[540] [541] [542] [543] [544] [545]			[540] [546] [547] [548]			[549]			

Table 8: Vulnerabilities Verses Sensors and Sources in Urban-Rural Driving Scenarios

HATS-PNT Subsystem	***Radar***	***GPS***	***INS***	***LTE***	***Camera***	***Lidar***	***WiFi***	***Legacy Maps***
Random walk Error			[552] [553] [554]					
Calibration Error			[552] [553] [554]					
Bias Instability			[552] [553] [554]					
Line of Sight	[555] [556] [557]	[558] [559] [560]			[561] [562] [563]	[564] [565]		
Low power signals	[566] [567]	[568] [569] [570]				[571] [572] [573]	[574]	
Multi-Path Reflection	[575] [576] [577] [578]	[579] [580] [581] [582]		[583] [584] [585] [586]	[587] [588] [589] [590]	[591] [592] [593]	[594] [595] [596]	
Atmospheric Layer Refraction		[597] [598] [599] [600]						
Weather	[601] [602] [603] [604]	[605] [606] [607] [608]		[609]	[610]	[611]		
Cloud/Fog	[612] [613] [614]	[615] [616] [617] [618]			[619] [620]	[621] [622] [623]		

Table 9: Threats Verses Sensors and Sources in Urban Rural Driving Scenarios

HATS-PNT Subsystem	***Radar***	***GPS***	***INS***	***LTE***	***Camera***	***Lidar***	***WiFi***
Eavesdropping				[624] [625] [626]			[627] [628] [629]
Denial of Service				[630] [631] [632]			[633] [634] [635] [636]
Sybil		[637] [638] [639] [640] [641]		[642] [643]			[637] [644] [645]
Black hole				[646] [647] [648]			[649] [650]
Reply Attack	[651] [652] [653]	[654] [655] [656]		[657] [658] [659]			[660] [661]
Timing		[662] [663] [664]		[657] [665] [666]			
Man in the Middle		[654] [667] [668]		[669]	[669]		[669]

Table 10: Threats Verses Sensors and Sources in Urban Rural Driving Scenarios

HATS-PNT Subsystem	***Radar***	***GPS***	***INS***	***LTE***	***Camera***	***Lidar***	***WiFi***
Spoofing	[670] [285]	[671] [672]		[673]	[674]		[675]
Jamming	[88] [676]	[677] [678]		[679] [673]		[129] [88]	[680] [677]
Physical Integrity	[681] [682] [683]				[684] [685]	[131] [655]	
Injection	[686] [687]	[688]		[689]	[690] [691]	[690] [131]	[692]
Impersona	[652] [693]	[694]		[695]	[696]	[697] [698]	[699]
Illusion	[700]				[701]	[129]	
Bogus information	[702]				[703] [536]	[704] [536]	

4 Vulnerabilities, Threats, and Mitigation for PNT Information in HAT Systems

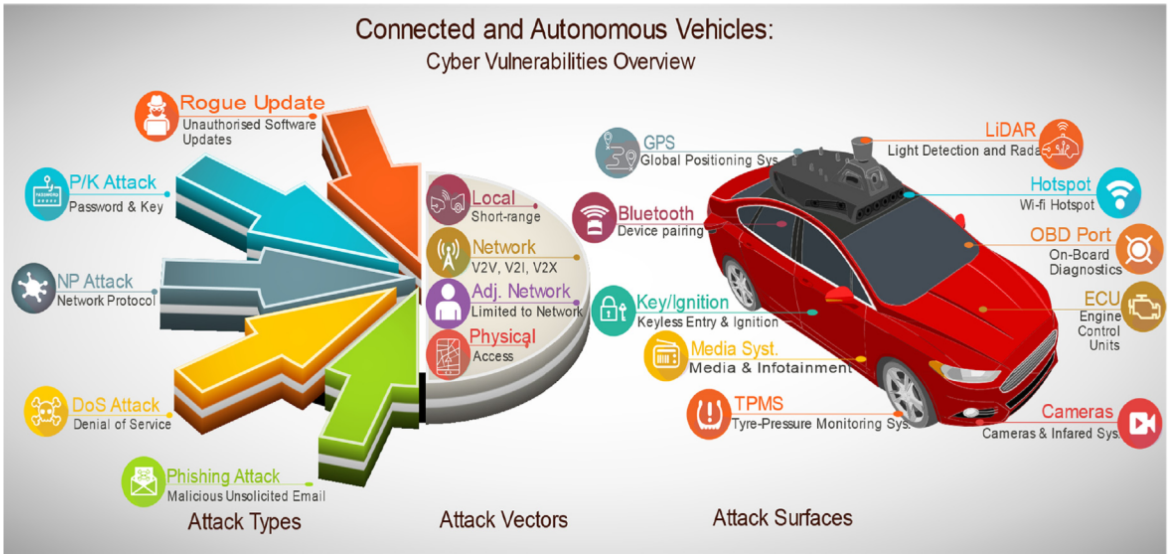


Figure 12: Attack types, Attack vectors, and Attack surfaces related to cooperative sensing and communication [705]

4.1 Roadside Sensing Technologies

In addition to the idea of cooperative sensing allowing for amplification of vehicles' situation awareness, other benefits are realized through the usage of sensor data from multiple vehicles or fixed roadside sensor stations. The functionalities offered by today's deployed technologies have the potential for significantly augmenting the capabilities of tomorrow's cooperative systems. Such capabilities offered by today's roadside technologies include [294]:

- Near-miss detection or trajectory projection, where for example a vehicle's dangerously close proximity to a pedestrian is alerted;
- Touchless crosswalks, where a pedestrian's intention to use a crosswalk is made known to a cooperative system;
- Detection of crosswalk violations
- As-needed crosswalk call extension (e.g., for disabled and elderly citizens)
- Call cancellation
- Call abbreviation (e.g., if someone is running or the crosswalk clears quickly)
- Driver notification of pedestrian mid-block crossings
- Crosswalk occupancy detection
- Automated and continuous turn counts
- Preemptive traffic signaling calls or vehicle behaviors to protect vulnerable populations, such as the elderly, schoolchildren, and those with disabilities
- Real-time data on what is around the corner for connected vehicle drivers
- Immediate incident detection and response

4.2 Sensor Fusion

The combination of different types of roadside sensing technologies through data fusion offers potential benefits to a cooperative system. One benefit is for the cooperative system to detect and adapt to the failure of a sensor, whether it be from a total malfunction (e.g. the sensor loses power), or from an environmental factor that exceeds the capability of a sensor's technology (e.g. too much solar glare that overwhelms a video input). Another benefit is to improve the possibility of achieving resiliency during a spoofing attack on one of the inputs.

Research has shown success in combining LiDAR data with a visual camera to address situations where the images are not clear, or the detections are unreliable. [706] trained a detector using a combination of optical images and their associated LiDAR 3D point clouds, captured at ranges of up to 50 meters. Object detection could be performed on the RGB images and the depths maps followed by the fusion of both results which lead to better detection performance compared to systems that rely upon only video. [707] also performed a similar investigation, but incorporated distance to the objects measured by the LiDAR as a relevant input to improve the classification performance. Accuracy of 97.2% was found with fusion, whereas video scored 96.2%. [708] followed a similar approach, but also included an added phase to track multiple pedestrians in a scene. The results demonstrate that the proposed method achieves significant performance improvement over a baseline method that solely uses image-based pedestrian detection.

4.3 Crowdsourcing

Several sensor-based technologies can be used for roadside applications to perform functions helpful for a cooperative system, such as those good for monitoring pedestrian volume and activity. However, it may not be feasible to install these kinds sensors all around a city [709]. Crowdsourced data can be used to help achieve required spatial and temporal coverage. Examples of crowdsourced data include those from smartphone apps (including map apps or fitness apps), passive Bluetooth or Wi-Fi sensing, and even social media. Most mainstream smartphones are now capable of generating huge volumes of social signals almost in real-time [710].

Several cities have begun to use data sources facilitated by the advancement in smartphone technologies to understand the route and time choices of pedestrians and identify pedestrian-dense origins and destinations. These data sources complement the traditional survey-based approaches that are used to collect information on walking activities and concentrations of pedestrians.

Crowdsourced data can be classified into active/explicit and passive/implicit sources depending on the level of input required from pedestrians. [711] defines passive data as those that need no or little interaction from users such as pedestrians and bicyclists, whereas active data require conscious input from users [711][712][713]. Passive data collection methods include Bluetooth/Wi-Fi, mobile phone positioning, global positioning systems (GPS), multi-app location-based services, and social media posts. Active data sources include fitness and tracking applications that require users to voluntarily access and set up the app to collect and store location data before initiating any trips.

Data analysis and provision companies purchase raw data from cellular carriers and application operators, clean and preprocess the data, apply algorithms that extract useful information, and sell the processed product. While crowdsourced data may not yield the same realtime capabilities or accuracy as those derived from on-vehicle or roadside GPS, video or LiDAR [714], they can be used for near real time safety purposes such as forewarning of drivers and automated systems of hazardous or anomalous conditions that can influence route choice analysis and crash exposure control. Beyond that, crowdsourced data can positively contribute to planning applications as travel demand estimation. Even so, crowdsourcing techniques continue to face numerous challenges regarding infrastructure, energy consumption, data quality, reliability, bias, accuracy, and privacy [713], [714].

4.4 Vehicle to Pedestrian (V2P)

We Investigated threats and vulnerabilities related to cooperative communication with Vehicle to everything (V2X) and Vehicle to Pedestrian (V2P) interaction. We studied threats and vulnerabilities related to V2X cooperative communication. V2X communication methods provide significant solutions for autonomous vehicles' perception and awareness. At the same time, it highlights important security concerns based on the form of communication in use. The information shared in this type of network is used in many automated driving tasks e.g., localization, decision-making, planning, and control. Therefore, attacks can change those tasks by manipulating the exchanged information which might lead to undesirable or hazardous driving behaviour. In [312], cooperative communication and sensing is tested for security threats in a connected vehicle stream in a Cooperative Adaptive Cruise Control (CACC) scenario. V2V communication is done wirelessly using IEEE 802.11p and used to share vital longitudinal control information among vehicles in a platoon setting. In this study, different attack surfaces are analysed with attacking methods like message falsification, spoofing, replay, jamming, eavesdropping, and tampering that are resulting in CACC instabilities and rear-end collisions. A study of different attack models and attack surfaces for autonomous automated vehicles and cooperative automated vehicles is conducted in [309]. In this work, threats and vulnerabilities related to V2I and V2V communication are identified for attack surfaces, such as infrastructure Roadside Units, security systems authority, and other vehicles to name a few, and assessed based on criteria that include means, feasibility, and severity of the attacks. The research work done by [715] explores most of the threats and vulnerabilities for autonomous and connected vehicles in the literature highlighting the attack types and knowledge gaps that are related to vehicles performing V2I and V2V communication in addition to different types of attacks on sensors and physical devices. Similar research is done in recent and more comprehensive studies by [716], [717] and [718] where threats and attack types are categorised based on the form of communication network that the autonomous vehicle utilises. Vulnerabilities of V2X communication technologies such as Vehicular Ad-hoc Network (VANET), which uses Dedicated Short-Range Communications (DSRC), are discussed in these studies with respect to its specifications and effects.

The purpose of V2P communication is to make Vulnerable Road Users (VRUs) and automated vehicles safer for all the stakeholders in the environment. VRUs include pedestrians, cyclists, and motorized two-wheelers. According to IRTAD, there were many fatalities of VRUs in 2017 [719]. Multiple works have been done to improve the safety of the VRUs. V2X is one such safety feature. V2X means vehicle to everything coopera-

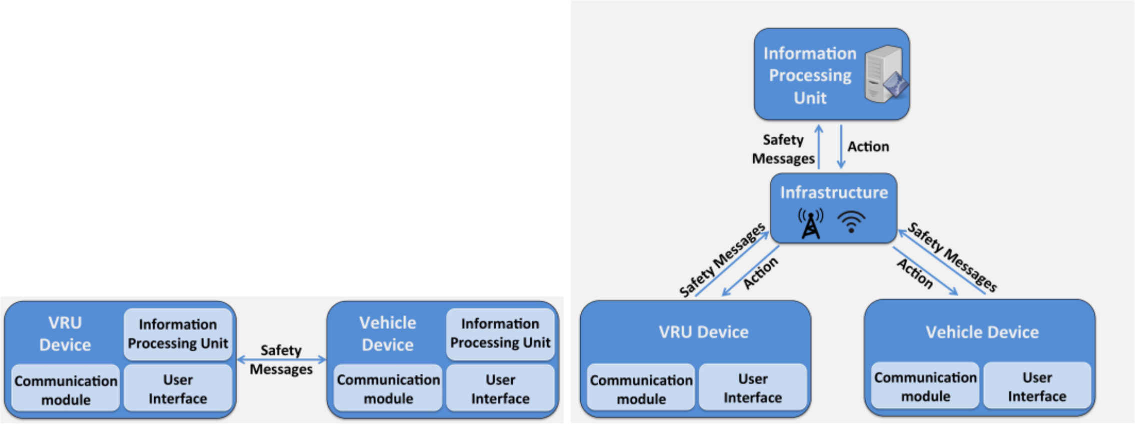


Figure 13: Direct Vs Indirect Communication Methods [720]

tive communication. It includes vehicle-to-vehicle V2V, vehicle-to-infrastructure V2I, and vehicle-to-pedestrian V2P cooperative communication. Since the focus here is on V2P, we will limit ourselves to threats and vulnerabilities related to V2P communication.

V2P system architecture for communication can be direct or indirect, simplex, half duplex, and full duplex Figure 13. For communication, we need transceivers on VRUs and vehicles and infrastructure if that is the chosen method for communication. The data transmitted is the location and speed of VRUs, which helps the vehicle detect, track and predict the trajectory of VRUs and then take collision avoidance maneuvers if necessary.

Due to the mode of communication established, V2P suffers from several vulnerabilities and threats. As for vulnerabilities, we have network congestion. as the number of VRUs and automated vehicles increases, network congestion can happen. Issue of network congestion is mentioned in [721]. To solve network congestion, methods such as using communication in simplex mode [722] clustering of VRUs [720] and transmission only when the threat of collision is predicted [721].

Another vulnerability is errors in location information, also called location accuracy. Location information is obtained by and large through GPS receivers. Other methods exist, but they are either not practical or cannot be deployed on a large scale. errors can be in range of anywhere between 3-50 meters depending on where is the GPS receiver (Urban/Rural), weather conditions clouds etc. [[722],[723],[724]]. Some efforts have been made to improve accuracy using Kalman filtering [725], and some other methods that give high accuracy [726]. Also, some things noteworthy here is that altitude information is critical when predicting trajectory. Current methods will predict a collision even when there is an overpass, and there is no chance of collision. Furthermore, some solutions to ignore GPS information if it has a high amount of error have also been developed. Entropy is used to assess the reliability of position information [727]. In this research, Kalman filtering-based data fusion is used to track, predict and monitor the location accuracy of HATS. An entropy-based metric is used to assess the reliability of the information. In another similar research, [728] multiple targets must be tracked with multiple dynamic sensing agents.

Mobile sensing agents plan their motion so that tracking can be efficient and accurate. An entropy-based cost function is utilized to reject information with an unacceptable variance.

In [725] a scenario is established where three types of vehicles exist on a highway. Namely, fully equipped, partially equipped, and not-equipped. A fully-equipped vehicle has local sensors and communication capability. In contrast, a partially-equipped vehicle can only communicate, and a not-equipped vehicle cannot communicate and does not have local sensors. The objective is to maintain a tracking list of all the vehicles present in the scenario with a tracking list in the partially and fully equipped vehicles. A Kalman Filter (KF) is used for data fusion and correction, and a covariance matrix generated through KF is used to measure the system's entropy. Data is rejected and considered unreliable if the entropy is beyond a threshold. This is used to determine location of occluded pedestrians in ”occupancy grid”
In case pedestrians are occluded, several methods are utilized to detect a pedestrian. In one method, using off-camera on the streets in an industrial area is used to detect the pedestrians through WiFi [729]. However, this solution is costly and not scalable. Another method by [730] utilizes software-defined radio to transmit the position of pedestrians that, in turn, is also very expensive as dedicated DSRC modules are too expensive. In [550] 802.11 b/g/n communication method is used so that HAVs can receive position information of occluded pedestrians, and the data is fused with LIDAR to get accurate results. However, this solution is also too expensive and not scalable. Currently, we do not have a vast network of WiFi routers in the road infrastructure. [731] used 3G/WLAN to communicate pedestrian information to the vehicle. However, it was not fast enough that the problem could become scalable and choke the network if the number of vehicles or pedestrians increased. With 4G/LTE and 5G, pedestrians can send their position information, and the communication modules are affordable. We suggest this communication protocol for sharing pedestrian location information with the vehicle. We have assumed all pedestrians have cell phones with GPS sensors available for pedestrian localization. The problem with GPS sensors is that it suffers from Non-Line of Sight (NLOS) in urban areas due to high-rise buildings and can have a high amount of position, navigation, and timing errors, which can have errors up to 50 meters. Also, GPS transmitting frequency can be easily generated, and fake information can be generated to misguide the sensor, resulting in accidents or unnecessary collision avoidance measures from the ego vehicle.

As many protocols can be used for communication with V2P. Each protocol have its pros and cons, such as WiFi and 4G/5G communication [732] and [733]. Standardization is required. Standardization of V2P protocols will pave the way for quick adaptation of V2P protocols in the real world.

As for threats, communication protocols can suffer from a wide range of attacks, such as spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. These attacks are also known as the STRIDE model [734]. In another research, [735], a complete threat model is presented to show possible threats and mitigation strategies. Mitigation strategies proposed are encrypted network protocols such as HTTPS and TLS, packet filtering, authentication, and others. However, these methods will increase latency within the network and expense for deploying the infrastructure required to implement V2P protocols. It is essential to mention that such threats are already identified in the previous sections of this report. However, they are significant to discuss from the perspective of threats related to V2P communication.

Some open research problems include but are not limited to 3D localization in V2P systems. Currently, there is no V2P protocol that is deployed in the real world on a large scale to observe the performance of automated vehicles. Limitations in tracking due to V2P communication protocol are unique as factors such as Time To Collision (TTC) and the nature of collision are unique for V2P systems and need to be explored. Integrating V2P with Geographic Information System (GIS) will also enable AVs to be cautious near an area where VRUs are expected. Furthermore, security-enhancing methods for threat mitigation need to be improved, as current methods might stall communication or delay communication which might result in collisions. Particular details of threats and vulnerabilities are mentioned in Table 8,9, and 10

5 Survey on Multisensor Fusion Localization: methods, attacks, detection and mitigation strategies

5.1 Introduction

Multisensor fusion is the process of combining information from multiple sensors to produce a more accurate and comprehensive understanding of a situation or environment. In the context of security and defense, this can be used to improve the accuracy of surveillance and detection systems, for example by combining data from GNSS, INS, radar, cameras, and other sensors to track and identify potential threats.

Stealthy methods for attacking multisensor fusion systems involve techniques that aim to evade or deceive these systems without being detected. By disrupting or manipulating the data from one or more of these sources, an attacker could potentially create confusion or uncertainty in the fused data, making it more difficult for the system to accurately track or identify potential threats. As such, it is important for designers and operators of multisensor fusion systems to be aware of these potential attack vectors and take steps to both detect and mitigate these threats.

This literature review focuses on analyzing multi-sensor fusion strategies, attacks, detection and mitigation mechanisms as found in the literature focusing on ground and aerial vehicles.

5.2 Multisensor fusion for localization

Modern Positioning, Navigation, and Timing (PNT) frameworks are extensively dependent on Global Navigation Satellite Systems (GNSS). Concurrently, GNSS-based PNT systems are progressively becoming more vulnerable to both accidental and intentional Radio Frequency (RF) interference. Specifically, with technology continually advancing and hardware costs reducing, minor efforts can significantly disrupt the standard functioning of nearly all PNT systems. This presents a significant threat to autonomous transport systems that depend on precise PNT.

With the expansion of communication capabilities, a cluster of vehicles operating in close proximity can readily exchange data. This allows for positioning and navigation based on a collectively computed navigation solution, often referred to as collaborative navigation. This potentially leads to a more accurate and dependable operation.

The utilization of sensors in autonomous vehicles presents potential risks when they are subjected to malicious manipulation or disruption. For instance, the GPS system, used for route identification, can be targeted by attackers through spoofing and jamming attacks. Spoofing involves the transmission of fabricated signals that deceive the GPS receiver, leading the vehicle in the wrong direction. On the other hand, jamming entails overpowering GPS signals, preventing the autonomous vehicle from receiving accurate positioning information.

The LiDAR system, constantly active in perceiving lanes, obstacles, and distances, is also vulnerable to attacks. Attackers can compromise LiDAR by transmitting spurious signals via a transceiver and introducing fake obstacles along the vehicle's intended path. This manipulation can cause significant misperception and jeopardize safety.

Furthermore, hackers can launch attacks on cameras used for obstacle detection, lane detection, and sign recognition. By directly targeting the cameras with laser light, attackers can blind the sensors, rendering them incapable of performing their intended functions. Such attacks can result in accidents on the road.

This review explores in detail the algorithms for MSF-based localization, cyber-physical attacks, detection and mitigation strategies. It also presents an evaluation of different standard-based approaches from Safety Engineering that can be used in addition to the aforementioned methods.

5.2.1 Background

Multisensor fusion localization design is a common approach that allows to fuse information from multiple independent sensors, such as GNSS, INS, LiDAR, etc. By combining data from multiple sensors, it is possible to overcome the limitations of individual sensors and improve the accuracy and reliability of the localization estimates [736, 737, 738, 739, 740, 741].

We refer to the system model in [742], that considers that the plan dynamics include a general model fault. This general model fault includes actuator faults, sensor faults and external attacks.

$$s(k+1) = As(k) + Bu(k) + B_a f_a(k) + \eta_1(k), \tag{1}$$

$$y(k) = Cs(k) + B_s f_s(k) + \eta_2(k) \tag{2}$$

Without loss of generality, we consider a general model of the 2D motion of a ground, maritime, or aerial vehicle, and model each vehicle as a discrete-time stochastic linear system with Gaussian noise. Thus, the state $s(k) = [p_x(k), v_x(k), p_y(k), v_y(k)]^\top \in \mathbb{R}^4$ represents the position $pos_s = [p_x, p_y]^\top$ and velocity $vel_s = [v_x, v_y]^\top$ of the vehicle in the 2D plane. The instantaneous velocity of the vehicle at any given time is $v_s = ||vel_s||$. The input consists of the accelerations in the 2D plane $u(k) = [a_x(k), a_y(k)]^T \in \mathbb{R}^2$, with instantaneous acceleration $a = \sqrt{a_x^2 + a_y^2}$. The output $y(k)$ represents the sensor or sensors measurement.

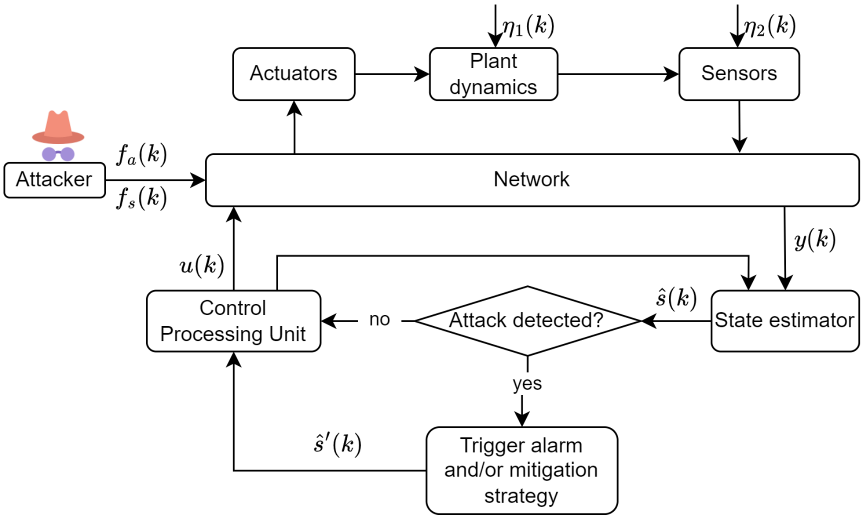


Figure 14: Cyber-attack detection and mitigation mechanism for the vehicle

Consider that the acceleration measurement by the internal plant model, INS/IMU has noise $\eta_1 \sim \mathcal{N}(0, \Gamma_1)$ and the sensor(s) measurement noise is $\eta_2 \sim \mathcal{N}(0, \Gamma_2)$. The attack sequences $f_a(k)$ and $f_s(k)$ are injected into the actuators and sensors of the system, respectively, and B_a, B_f are the corresponding matrices of appropriate dimensions.

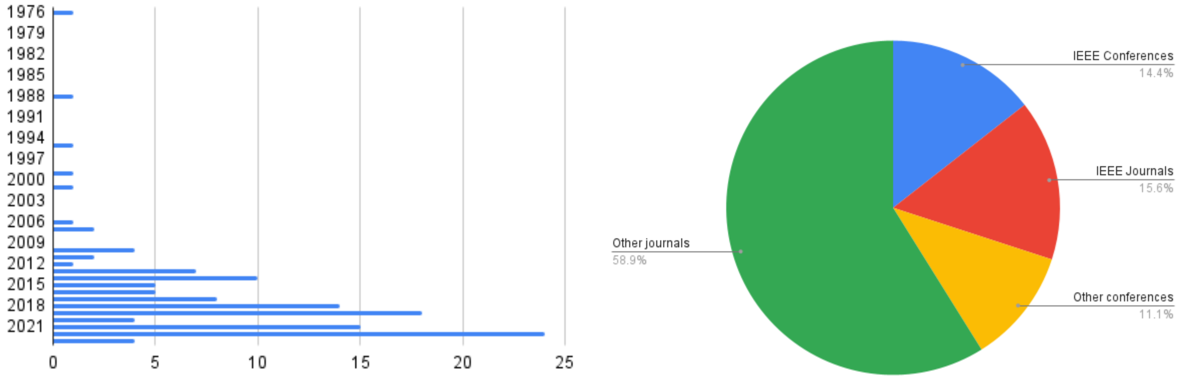
Then, the workflow for the attack and detection follows as in Figure 14. The attacker inputs the actuator or sensor attack sequences $f_a(k)$ and $f_s(k)$ into the network layer of the system to attack actuators and/or sensors. Then, the output measurements of the sensors are sent through the network layer to the state estimator. The location estimates from each sensor are combined using a fusion algorithm, such as a Kalman filter, particle filter, weighted average or a maximum a posteriori, to provide a more accurate and robust estimate of the object's location. The output of this estimation is send to the detection mechanism that compares against previous outputs of the system, previous estimations or calculates the covariance in the evolution of the output, and identifies whether the system is under attack. If it is, an alarm is triggered and a mitigation strategy may be incorporated to compensate for the attack.

When having multiple sensors, it is usual to have more than one estimation method and detector. The compensation is then done by selecting the output of the estimate algorithms that fuse the information from the sensors that are not under attack.

5.3 Taxonomy

The proposed taxonomy for this literature review attempts to identify the most important characteristics of the multisensor fusion-based localization algorithms and attack detection as follows:

- **MSF estimation methods for localization**: methods proposed by researchers to esti-



(a) Distribution by year of publication.

(b) Distribution by type of publication

Figure 15: Overview of the reviewed works.

mate the location of a vehicle or group of vehicles.

- **Cyber-physical attacks overview**: types of attacks that can interfere with the normal operation. We review types of attacks based on stealthiness and objective.
  - **Stealthiness**: these attacks can be covert or overt with a subclassification for each.
  - **Objective**: we revise different types of attacks depending on the goal of the attacker.
- **Attack detection**: statistical methods and optimization based methods to identify when the system is under attack. This includes detecting the source of the attack and trigger an alarm or a mitgation strategy.
- **Mitigation strategies**: overview of approaches in the literature to react when an attack is detected.
- **Risk assessment strategies**: approaches to qualitatively and quantitatively assess safety for autonomous systems.

Around 90 papers were reviewed, additional references come from the press, books, dissertations, standards or testing procedures released by state agencies. From the reviewed papers, 30% come from either IEEE journals or conference proceedings, and 11.1% come from other type of conference proceedings and 58.9% are from other journals as shown in Figure 15b.

We have placed more emphasis in recent work, with 88% of the reviewed works published in the last decade. A distribution of the years and number of works reviewed is shown in Figure 15a.

5.4 MSF estimation methods for localization

In a system that has multiple sensors, each sensor will have its own unique measurement characteristics, error, biases and noise. Hence, the measurements from different sensors are not necessarily consistent with each other. Furthermore, they may measure different variables (distance, angle, speed) that are related to localization, but do not directly provide it. Then, using estimation methods allows to optimally combine the data from the sensors and achieve the most accurate location estimation possible. The purpose of estimation methods is to take the measurements of the sensors along with a model of the system dynamics and the statistical properties of the sensors' errors and biases, and provide the best estimate of the system's state, which includes its location. Some of the most common estimation methods are the following.

- Kalman filtering: This is a recursive algorithm that uses a statistical model to estimate the state of a system based on noisy, incomplete, or uncertain data from multiple sources. It is commonly used in sensor fusion for localization because it can effectively combine data from multiple sensors and account for errors or uncertainties in the data.
  - **Linear Kalman Filter**: this is a closed-form solution to the linear Gaussian filtering problem that requires to assume that the model is a linear and Gaussian. By simplyfing the vehicle motion to a linear model, a good estimate of the localization is obtained in [743, 744, 745, 746, 747, 748, 749]. These works perform fusion of IMU/INS information and GPS/GNSS data.
  - **Extended Kalman filtering**: This is a variation of Kalman filtering that is used when the system being modeled is nonlinear. It uses a linear approximation of the nonlinear system to estimate the state of the system based on the data from the sensors. EKF is prominently featured in about 50% of the reviewed works, often in combination with other supplementary techniques. The advantage of EKF over KF is that it can handle nonlinearities in the system, and the advantage of EKF over UKF, it that it is still relatively simple to implement [750, 751, 752, 753, 754, 755, 756, 757].
  - **Unscented Kalman filtering**: This is a variation of Kalman filtering that is used when the system being modeled is nonlinear, but the nonlinearities are not well-known or cannot be accurately modeled. It uses a set of carefully chosen points, or sigma points, to propagate the state of the system through the nonlinearities and estimate the state of the system based on the data from the sensors [758, 759, 760].
  - **Modifications to KF, EKF and UKF**: Among the several variants of Kalman Filter are the switching Kalman Filter [761], iterative EKF [762], interactive multiple model with EKF [763], error state KF with delay handing [743].
- **Particle filtering**: This is a Monte Carlo-based algorithm that uses a set of weighted particles to represent the state of a system. It can be used to estimate the position of an object or system by updating the particles based on the data from the sensors, and then using the weighted particles to compute the most likely position of the object or system. This method has proved its effectiveness in addressing the bias introduced by GPS in

[764, 765]. A particle filter that includes fusion with probabilistic maps for changing ODD conditions is also proposed in [766]

- **Graph-based optimization**: This is a technique that represents the localization problem as a graph, where the nodes of the graph represent the sensors and the edges represent the relationships or constraints between the sensors. The goal of the optimization is then to find the best possible configuration of the nodes on the graph that satisfies the constraints and produces an accurate estimate of the object's position. Mascaro et al. proposes to use this method to fuse the visual inertial odometry poses and the globally referenced positions to infer the global localization of UAVs in real-time [767]. In [768], an asynchronous graph optimization method is proposed to incorporate sensors that operate at different sampling rates.

- **Machine learning-based localization**: This is a technique that uses machine learning algorithms to learn from data and improve the accuracy of the localization estimate. It can be used to learn the relationships between the data from the sensors and the position of the object or system, and can be particularly effective at handling complex, nonlinear localization problems. For example, the A3C algorithm combined with EKF has shown to enhance localization accuracy [756]. Another novel approach is the application of Convolutional Neural Networks (CNN) to estimate maritime vessel positions [769]. However, maritime and especially underwater vehicles face additional challenges due to the lack of GNSS signal underwater. Zhao et al. [770] leverages a Bayesian network for precise vehicle localization and road matching.

Alternative approaches to handle localization when GPS is under attack include modeling localization error based on probabilities [771], voxel-based matching [772], and using EKF with alternative sensors like IMU+Camera [736] or IMU+LiDAR [737]. Cooperative localization by leveraging GPS and V2V/V2I shows robust performance for localization in [773]. A particle filter estimator is combined with a CNN for increased UAV localization accuracy in [774].

Methods incorporating additional sensors for localization often employ variations of the Kalman Filter like EKF or UKF, usually in combination with another method to fuse information from cameras [775], LiDAR [776] or maps [777]. When LiDAR and no GNSS/INS are involved, probabilistic state estimators are usually used to fuse wheel odometry data and images from a monocular camera with a predefined map [778, 779]. A summary of the combination of sensors used per MSF estimation method is given in Table 11.

5.5 Cyber-physical attacks overview

In the context of attacks, the localization stack of the vehicles is often targeted. We focus on threats targeted toward the sensors, actuators and controllers of the vehicles, namely, their cyber-physical layer. There are also physical attacks that include physically damaging or disabling sensors or placing obstacles in the environment that could affect per-

Table 11: Commonly used MSF methods and associated sensors.

Reference	Sensors for localization									Cooperative	Type vehicle	MSF
	GNSS	INS	IMU	Radar	Lidar	Camera	Map	V2I/V2V	Odometer			
[766] Levinson (2011)	✓	–	✓	–	✓	–	✓	–	–	–	🚗	PF
[764] Jo (2013)	✓	–	✓	–	–	–	✓	–	–	–	🚗	PF
[780] Carson (2016)	✓	–	–	–	–	–	–	–	–	✓	🚗	Cooperative DR
[781] Hardy (2016)	–	✓	–	✓	–	✓	–	–	–	✓	✈	EKF, UKF
[763] Glavine (2018)	✓	✓	–	–	–	–	–	–	–	–	🚗	EKF
[743] Wan (2018)	✓	–	✓	–	✓	–	–	–	–	–	🚗	EKF
[778] Bürki (2019)	–	–	–	–	–	✓	✓	–	✓	–	🚗	Probabilistic
[782] Liu (2019)	✓	–	✓	–	✓	–	–	–	–	–	🚗	EKF
[738] Shen (2020)	✓	✓	–	–	✓	–	–	–	–	–	🚗	EKF
[769] Grelsson (2020)	–	–	–	–	–	✓	✓	–	–	–	🚢	ML-based
[783] De Miguel (2020)	✓	–	–	–	✓	–	✓	–	–	–	🚗	Probabilistic
[779] Cao (2020)	–	–	–	–	✓	–	✓	–	–	–	🚗	Graph optimization
[762] Liu (2021)	–	–	✓	–	–	✓	–	–	–	–	🚗	ML-based, EKF
[756] Zhang (2021)	✓	–	–	–	–	–	–	–	–	–	🚗	RL-based, EKF
[784] Yousuf (2021)	✓	✓	–	–	–	–	–	–	✓	–	🚗	ML-based, KF
[777] Viana (2021)	✓	✓	–	–	✓	–	✓	–	✓	–	🚗	NDT-EKF
[785] Zahedian (2021)	–	–	–	–	–	✓	–	–	–	–	🚗	KF
[786] Ding (2021)	✓	–	–	–	–	✓	–	–	–	✓	✈	Cooperative DR
[787] Zhang (2021)	✓	–	✓	–	–	–	–	–	–	–	🚗	EKF, UKF
[788] Wang (2021)	✓	–	–	–	✓	–	–	–	–	–	🚗	EKF
[737] Marković (2022)	–	–	✓	–	✓	–	–	–	–	–	✈	EKF
[736] Yan (2022)	–	–	✓	–	–	✓	–	–	–	–	🚗	EKF
[771] Zhang (2022)	–	–	✓	–	–	–	–	–	–	–	🚗	Error modeling
[772] Shen (2022)	–	–	✓	–	✓	–	–	–	–	✓	✈	CV-based
[773] Shan (2022)	✓	–	–	–	–	–	–	✓	–	✓	🚗	EKF
[775] Kim (2022)	–	–	✓	–	✓	–	–	–	–	–	🚗	NDT-EKF
[776] Xia (2022)	–	–	–	–	✓	–	✓	–	–	–	🚗	NDT-EKF
[755] Wu (2022)	✓	–	✓	–	✓	–	–	–	–	–	🚗	EKF
[789] Afifi (2022)	✓	–	–	–	–	–	–	–	–	–	🚗	FKF
[790] Torroba (2022)	–	–	–	–	✓	–	–	–	–	–	🚢	SVGP
[791] Liang (2022)	✓	✓	–	–	–	–	–	–	–	–	🚗	EKF
[792] Dares (2022)	–	–	✓	–	✓	–	–	–	✓	–	🚗	EKF, UKF

ception, but we do not cover this topic. To facilitate analysis and categorization, two key classifications are introduced: stealthiness and objective of the attack.

5.5.1 Classification based on Stealthiness

We can classify the attacks as follows according to [146]:

- **Overt**: these are attacks that are mostly visible and easily detectable, whose purpose is to cause disruption and send a clear message. Types of overt attacks are Denial of Service (DoS), their derivatives such as Distributed DoS and jamming (usually overt, but there can be instances when it is designed to be covert). If the attack is only on the actuators, it can only be overt as the estimation error is bounded [793].
  - **Denial of Service (DoS):** DoS attacks prevent sensor readings from reaching the destination, hence the sensor measurements cannot be updated and the last observation would be considered as the current one. This type of attack is implemented in [788] and compared against False Data Injection, stealthy attack and replay attack. Also Liu et al. [762] implements it to measure the performance of its LSTM+EKF estimator.

  - **Jamming**: involves using electronic signals to interfere with or disrupt the signals from the sensors, making it more difficult for the system to accurately estimate the position of an object or system. GPS blockades of 10s are proposed in [777] to attack the system with a NDT-EKF estimator.

- **Covert**: these are attacks that are stealthy and their purpose is to remain undetected as their pursue the objective of infiltrating a system, gaining information or leading the system to a malicious destination. If the attack is on the sensors, or in the sensors and actuators, it has been shown that the estimation error can be unbounded, hence covert [793].

  False Data Injection (FDI) is a common covert attack in networked systems. FDI attacks are a common type of attack that aims to manipulate a system's handling of sensor measurements by introducing manipulated measurements into the system's sensors, for example in smart grids [794, 795], sensor networks [796, 797] and nonlinear systems in general [798]. Within FDI we find specifically for localization systems of vehicles the following subtypes:

  - **Spoofing**: involves creating false signals or data that is designed to deceive the sensors, leading the system to estimate an incorrect position for the object or system. Spoofing is usually covert, but there can be instances when it is designed to be overt. Furthermore, it was also shown that an attack designed with an open-loop spoofing controller is more likely to stay covert than attacks produced by a closed-loop controller [146]. According to [799] we can consider three common GNSS spoofing techniques according to their sophistication level: simplistic, intermediate and sophisticated. The works analyzed in this review belong to the simplistic (can be overt) and intermediate level (covert), as the sophisticated spoofing attack involves using multiple receiver-spoofer devices that target the receiver from different angle and directions, and it is considered that the only successful defense against this type of attack is cryptographic authentication [800].

    A simple way of spoofing a sensor would be to insert bias as in [764]. Another method used to design attacks for KF estimators includes introducing noise or signals that are statistically similar to legitimate signals that are to be estimated using the KF [146, 801, 802, 803, 804]. Some robust spoofing attacks on the GNSS of aerial vehicles are designed to evade fault detectors in the multisensor fusion filter, thereby posing a potential single point of failure [801, 802]. The target GPS unit or receiver is deceived in [805] by duplication or falsifying GPS signals. LiDAR spoofing attacks can process point cloud data to add virtual obstacles or remove obstacles in real scenes [129]. In [87], the attacker remotely disrupts a LiDAR based autonomous vehicle by generating more object and vehicle echoes. A minimization based spoofing attack for ships via false GPS signals is proposed in [806].

  - **Replay attacks**: do not need any system information, but rather the attacker records a sequence of sensor observations and replays the sequence afterwards. Since the data comes from real recordings and satisfies the mathematical models of the vehicle, it can be more deceptive than other attack methods. A LiDAR replay attack is proposed in [782] and a general replay attack is used for devising secure fusion estimation in [807].

  - **Meaconing**: consists on inserting delayed signals by intercepting and then rebroadcasting them causing a time-drift for the sensor (usually a GNSS) [808, 805].
  - **Time alteration attacks**: consists on altering the sensor signal by modifying its timestamp or changing the time propagation of the signal to the receiver [809, 805]

5.5.2 Classification based on Attack objective

For a complete takeover, according to Sathaye *et al.* [810], the attacker should be able to control the speed or direction of the victim, or force it to stop (ground vehicle) or land (aerial vehicle). Achieving the attacker's goal largely depends on the spoofer's capabilities and the victim's anti-spoofing features [805]. By grouping by attack objective, we have the following.

- **Deviating Attack:** the attacker guides the victim to follow a wrong route, to prevent if from reaching its destination, cause delays or confusion. In [738], a minimization based function is proposed to force the ground vehicle go off-road and to go the oncoming lane. Other works that take a similar approach for ground vehicles is [811] and for aerial vehicles [810]. This last work also proposes to use a human in the loop GPS spoofer (HITL), where the human attacker observes the UAV's motion and manipulates the trajectory through a human interface device.
- **Targeted Attack:** the attacker guides the victim to a specific destination.
  - **Malicious destination:** when the victim arrives to the malicious destination, it would be subject to ambush, robbery or theft. Su et al. [802] proposes a design for the residual so that UAVs are directed to a malicious destination without triggering the residual based detector. Zeng et al. [811] proposes a stealthy attack to road navigation systems where the goal is to trigger the fake turn-by-turn navigation to guide the victim to a wrong destination without being noticed by slightly shifting the GPS location so that physically feasible instructions are generated. This study found that 95% of the participants followed the navigation to the wrong destination without recognizing the attack.
  - **Endangering:** the attacker guides the victim into a dangerous situation, such as entering the wrong way on a highway. The work of [738] also fits within this category.
  - **Destruction:** the attacker sets the victim on a collision course with an obstacle or the ground. In this case, it is challenging to make the attack stay covert, as other subsystems of the vehicle may raise flags regarding imminent collision. Mendes et al. [812] found that through a combination of attacks, crashing a commercial quadcopter was possible most of the times due to their lack of security properties.

As also noted in [813], we have found that most studies focus on defining attacks rather than considering defense mechanisms. Hence the following two sections will explore the challenges of attack detection and attack mitigation, which can go together, but not necessarily.

5.6 Attack detection

Prior studies often overlook the full range of nonlinearities in vehicles and the adverse effects of malicious disturbances, resulting in reduced control performance and instability [814]. Neglecting the security measures in sensor design for autonomous vehicles is a significant vulnerability, as cyber-attacks can compromise the safe operation of the vehicle, possibly leading to accidents and being a menace to users.

As shown in [815] one can understand that attacks are designed in general for cyber-physical systems, and similar types of attacks can affect power grids, vehicles, network systems, etc. Then, one can *borrow* methods from those other fields too.

Outlined in [742], a residual signal can be produced by utilizing the input vector $u(k)$ and output vector $y(k)$, such that $r(k) = g(u(k), y(k))$. Typically, this residual signal $r(k)$ represents the discrepancy between the measured output $y(k)$ and the estimated output $\hat{y}(k)$, as expressed by the following equation:

$$r(k) = y(k) - \hat{y}(k) \tag{3}$$

The residual signal exhibits the following attributes:

- Invariance Relationship: In the absence of any faults, the mean of the residual signal $\mathbb{E}[r(k)]$ equals zero.
- Fault Detectability: In the presence of any faults (such as sensor or actuator attacks, noise interference, etc.), the mean of the residual signal $\mathbb{E}[r(k)]$ becomes unequal to zero.

Furthermore, if there are no cyber-attacks, the residual has a zero mean Gaussian distribution with a constant covariance matrix $\Sigma_r(k) = C\Sigma(k)C^\top + \Gamma_2$ and $r^\top(k)\Sigma_r^{-1}(k)r(k)$ follows a χ^2 distribution with n degrees of freedom, where $\mathbb{E}[r^\top(k)\Sigma_r^{-1}(k)r(k)] = n$. The dimension of the measurement vector $y(k)$ coincides with dim$(s(k)) := n$, i.e. dim$(y(k)) = n$. A general outlier detector using χ^2 consists on triggering an alarm or flag when χ^2 goes above a threshold, as shown in [816, 817, 818, 797].

Then, to detect whether the system is under attack, one can use statistical hypothesis testing methods such as the Cumulative Sum (CUSUM) [819], Compound Scalar Testing (CST) [820], sequential probability ratio test (SPRT) [821] and generalized likelihood ratio

(GLR) [822]. This last method was initially proposed in [823]. This statistical analysis will be the tool for decision making (accept or reject the hypothesis will lead to raising a flag that shows attack). Even though χ^2, CUSUM, CST, SPRT and GLR detectors are effective in detecting faults or attacks such as denial of service attacks, short-term randomized attacks, and long-term randomized attacks, they are unable to detect statistically derived false data injection attacks [794].

In the case that the system uses a KF estimation method, there are some commonly used approaches for detecting false data injection attacks. In [782], the authors consider two types of attacks: GNSS spoofing and LiDAR replay attack, and the designed detector is based on monitoring the cumulative sum (CUSUM) of the residual, similar as proposed in [146, 801, 802]. In the case of multi sensor fusion, it is common to design different combinations of EKF and the CUSUM detector, so that the attacked sensor can be identified, as shown in [782, 824, 788].

A linear filter is proposed to detect the sensor shift or shift in the system matrix A and the control matrix B. Then, the gain of such filter is modified to make the residue of the filter more sensitive to a shift [825, 826]. Roysdon et al. [827] considers MSF between GPS and INS, and proposed to use a sliding window filter for outlier detection and elimination. Some authors propose other models to detect cyber-attacks. For example, [828] uses the error vector to detect cyber-attacks, with the error value of the *n*th EKF directly.

Even though using EKF and its derivatives for estimation is the most and used method as it provides robustness in performance, they are subject to cybersecurity attacks and the attack defenses and mitigation strategies is still a developing subject. Some works that look into this topic are in adjacent fields to transportation, mostly in the area of networked nonlinear systems. For example, in [829] the authors propose modified particle filters for detection of false data injection attacks. A similar method is proposed in [830], but the application is in automatic generation control systems.

Methods for detecting cyber-attacks on UAS include monitoring error vectors of Extended Kalman Filters (EKF) to compare sensor values [814], combining different detection strategies for spoofing attacks [824], and monitoring discrepancies between GNSS-derived measurements and corresponding sensor readings [831].

Other methods resort to using tools from anomaly detection. In [808] the authors use a Support Vector Machine (SVM) approach to detect GPS spoofing. In the case of a meaconing attack, some authors suggest to monitor the receiver's clock drift [832].

5.7 Mitigation strategies

It has been shown that combining several spoofing detection methods leads to a more robust detection, furthermore, one can identify also different kinds of attack, such as in [824]. In this case, the mitigation method is to use the sensor fusion approach just using the sensors that are not being attacked, i.e. if the detector finds that the GPS is being attacked, use the EKF that fuses LiDAR and IMU information.

Some localization algorithms include anti-spoofing or anti-attacks safeguards. For example, in [791] the authors propose an anti-spoofing Kalman filter for GPS/INS sensor fusion. However, this work requires a pregenerated map of the environment, obtained using SLAM. Applications of this method were initially used for mobile robots, and lately for automated vehicles.

UKF-based pose estimation methods have shown promise in handling challenges such as bandwidth constraints and randomly occurring deception attacks [833, 807, 804] with the only downside of being more complex to implement.

In [834], the author proposes a probabilistic map that increases the robustness of the localization using particle filters when having the availability of GPS, IMU and a map.

A common anti-spoofing method for GPS information is usually carried out by testing the variance of the error in the measurement from one timestep to the next one. In [791] for example, this method was used. However, as shown in this work, small increases in the spoofing error are not detected by this method and can lead to cumulative errors in the total time of simulation.

Mitigation strategies for replay attacks include robust filtering methods, such as the recursive distributed Kalman filter that is proposed in [807].

Other studies have focused on studying the advantages of collaborative navigation for detection and mitigation of GNSS-based PNT anomalies. For example, in [835] an outlier detection method is used. Minimum Norm Least Squares Solution (MINOLESS) is selected in this study because the solution norm is minimized among all possible (biased) solutions. By incorporating this solution, the collaborative navigation has shown to be able to maintain the differences to the reference solution to within 0.2 m for the biased case, 0.5 m for the noisy case and 3 m for the anchor case.

Moreover, multisensor information fusion algorithms such as Gaussian Processes, evidence theory, and the improved CNN algorithm potentially enhance estimation accuracy and robustness against cyber attacks [836, 837].

5.8 Risk assessment strategies

There are several approaches to qualitatively and quantitatively assess safety, many of them are founded on standards that dictate the expected behavior of systems under certain configurations. The Road Vehicle Functional Safety standard (ISO 26262) [838] considers that hazards that are induced by software or hardware failures. The Road Vehicle Safety of the Intended Functionality standard (SOTIF ISO/PAS 21448) [839] seeks to identify performance shortcomings in ADAS systems that may occur not because of a system failure but rather due to limitations in the nominal system performance. A recently introduced standard, the UL4600: Autonomous Vehicle Safety Standard [840], consists of safety definitions for autonomous systems specifically. Fig. 16 shows the three main categories for safety assessment: Systems Engineering methods, formal methods, and probabilistic methods. These methods can also be classified according to their outcome, such as Hazard analysis, Safety Case Specification, and Risk Assessment methods.

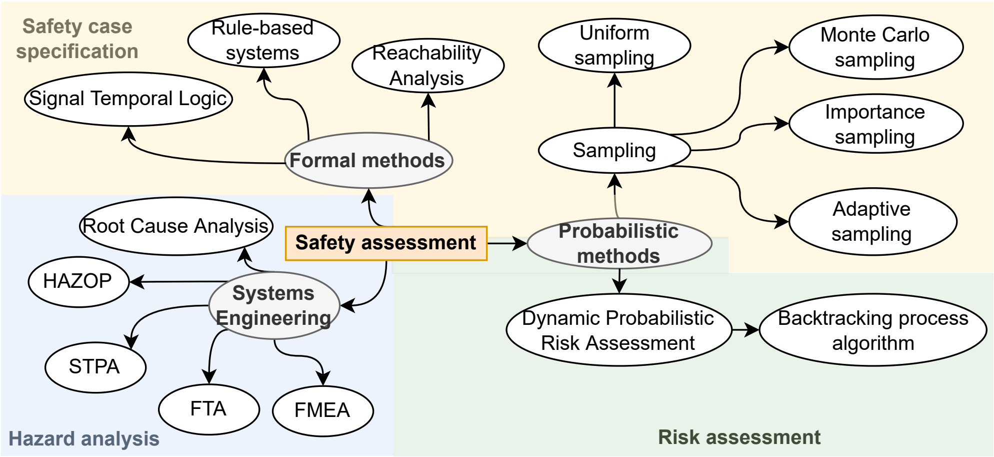


Figure 16: Some safety assessment methods explored. Notice that the main areas: Systems Engineering, Formal Methods and Probabilistic Methods comprehend a series of analysis procedures that have different goals. Systems Engineering Methods are used for Hazard analysis, Formal methods and Sampling-based methods are used to build the safety case specification and some Probabilistic methods are used for risk assessment.

Systems Safety Engineering methods provide systematic methodologies to perform Hazard Analysis. The traditional Fault Tree Analysis (FTA) and Failure Modes and Effects Analysis (FMEA) consider that hazards result from chain events caused by individual components' failures propagating throughout the system. The difference between both methods is that FMEA uses a bottom-up cause-effect model while FTA is an top-down effect-cause approach. Hazard and Operability Study (HAZOP) is a qualitative top-down hazard analysis method for complex systems that consists of evaluating each component in a chain process and finding potential situations that would provoke hazards. System Theoretic Process Analysis (STPA) [841] provides a systematic process to evaluate interfaces between system components, controllers and people, using process feedback loops, functional control diagram, system requirements, hazard scenarios, safety constraints and safety requirements.

Previous studies have shown that the combination of two or more hazard analysis methods leads to better identification of potential hazards and mitigation strategies [842, 843, 844, 845].

The application of hazard analysis techniques to an automotive PNT subsystem is not new. Brewer et al. [846] presented a very detailed STPA+HAZOP+FMEA analysis for a generic automated lane centering system. Similarly, Becker et al. [842], developed the same analysis for a generic SAE level-3 highway chauffeur system, including lane changing and lane centering maneuvers, while Koelln et al. [847] presents the STPA comparison in general for a vehicle SAE level-4 and level-5. Mahajan et al. [844] presents an STPA for a lane-keeping assistance system, while Abdulkhaleq et al. [848] applies STPA to the lane change functionality of a cruising chauffeur. Macher et al. [849] introduced a security aware hazard and risk analysis method whose focus is in newer electronic devices. It is a combination of the automotive Hazard Analysis and Risk Approach (HARA) and the security domain STRIDE approach that allows identifying computer security threats. Sulaman [850] makes a comparison of the outputs of a forward collision avoidance (FCA) system using FMEA and STPA. Unlike other works mentioned in this section, the analysis is carried out independently using each hazard analysis method, and the outputs are compared qualitatively. However, as explained in [847, 842], it is more effective to combine methods instead of using them independently.

Capito *et al.* developed a workflow pipeline that can be used for risk assessment using hazard analysis methods, as shown in Fig. 17 [851]. Here, the analysis goes directly from the item definition to the risk assessment without further iteration.

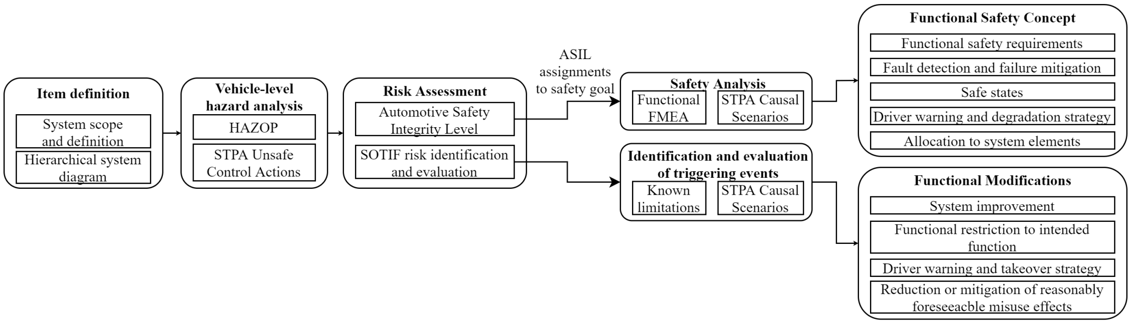

Item definition
System scope and definition
Hierarchical system diagram
Vehicle-level hazard analysis
HAZOP
STPA Unsafe Control Actions
Risk Assessment
Automotive Safety Integrity Level
SOTIF risk identification and evaluation
ASIL assignments to safety goal
Safety Analysis
Functional FMEA
STPA Causal Scenarios
Identification and evaluation of triggering events
Known limitations
STPA Causal Scenarios
Functional Safety Concept
Functional safety requirements
Fault detection and failure mitigation
Safe states
Driver warning and degradation strategy
Allocation to system elements
Functional Modifications
System improvement
Functional restriction to intended function
Driver warning and takeover strategy
Reduction or mitigation of reasonably foreseeacble misuse effects

Figure 17: Safety Analysis and Requirements Development Process

The analysis consists of systematically performing a detailed expert-based evaluation of every component of the system using the hazard analysis tools described above. The output of the analysis is a series of tables that describe the potential level hazards, their ASIL rating for risk assessment, safety goals, triggering events and mitigation strategies [851]. The disadvantage of expert-based methods is that it is possible to generate very different outcomes depending on the extent of the considered ODD and the knowledge and experience of the particular subject matter experts. Nevertheless, it remains a valuable resource to find possible adversarial disturbances applied to the test-subject.

In comparison, the authors of [852] propose a Hazard Based Testing approach derived from STPA, where the testing miles reflect hazard-based scenarios that are relevant to the way how an ADS fails.

A comparison of the aforementioned methods is shown in 12. We can see that there are mostly qualitative methods as quantitative methods purely from systems engineering need to be combined with others such as formal methods. Some quantitative methods that do not borrow from systems engineering are probabilistic risk assessment algorithms [853, 854], fuzzy logic methods [855] and Monte Carlo approaches [856].

Table 12: Risk assessment approaches for automated driving systems

Reference	Method								Quant/Qual	ISO 26262	ISO/PAS 21448
	STPA	FTA	FMEA	HAZOP	HARA	ASIL	DRA	QRN			
[842] Becker (2020)	✓	✓	✓	–	–	–	–	–	Qualitative	✓	✓
[857] Capito (2021)	✓	–	✓	✓	–	✓	–	–	Qualitative	✓	✓
[858] Warg (2016)	–	✓	–	–	✓	–	–	–	Qualitative	✓	–
[859] Stolte (2017)	–	–	–	–	✓	✓	–	–	Qualitative	✓	–
[860] Bagschik (2016)	–	–	–	✓	–	✓	–	–	Qualitative	✓	–
[861] Wardzinski (2008)	–	–	–	–	–	–	✓	–	Qualitative	–	–
[862] Khastgir (2017)	–	–	–	–	✓	✓	–	–	Qualitative	✓	✓
[863] Warg (2020)	–	–	–	–	✓	–	–	✓	Quantitative	✓	✓
[864] Puch (2018)	–	✓	–	–	–	–	✓	–	Quantitative	–	–

5.9 Discussion

This document provides a general review of methods for locating, attacking, and mitigating threats to ground, aerial, and maritime vehicles. However, additional considerations, unique to each vehicle type due to their operational design domains, are beyond the scope of this review.

The operating environment presents distinct vulnerabilities. Ground vehicles are susceptible to physical attacks, including tampering with sensors or cameras. Aerial vehicles may succumb to signal interference, causing loss of control or crashes. Maritime vehicles may experience attacks on their propulsion system, such as clogging of their water intake. Further, while 2D motion is an adequate approximation for ground and maritime surface vehicles, it is insufficient for aerial vehicles and maritime underwater vehicles. As noted in [810], GNSS spoofing alone cannot alter the altitude of an aerial vehicle to force a landing, as most such vehicles rely on non-GNSS sensors (rangefinders, downward-facing cameras, barometers) for altitude measurement. These sensors' immunity to GNSS spoofing presents a significant challenge for attackers.

Sensor configurations also vary among vehicles. Ground vehicles heavily depend on LiDARs, susceptible to laser interference, or cameras, vulnerable to spoofed images. Aerial and maritime vehicles may contend with sensors that depend on environmental factors, such as barometric pressure sensors disrupted by weather or altitude changes, or sonar sensors disrupted by waterborne debris.

Risk assessment strategies should take into account that different types of vehicles may fall under various regulatory frameworks or security standards, influencing the relevant attacks and required mitigation strategies.

Furthermore, the medium for data storage and transmission used by vehicles deserves consideration. For instance, ground vehicles may store data locally, whereas an aerial vehicle might transmit this data in real-time to a remote server.

Overall, this research area is rapidly expanding, driven by increasing sensor use in ground, aerial, and maritime vehicles and escalating levels of vehicle automation.

References

[1] Z. Clements, P. A. Iannucci, T. E. Humphreys, and T. Pany, “Optimized bit-packing for bit-wise software-defined GNSS radio,” in *Proceedings of the ION GNSS+ Meeting*, (St. Louis, MO), 2021.

[2] H. A. Nichols, M. J. Murrian, and T. E. Humphreys, “Software-defined GNSS is ready for launch,” in *Proceedings of the ION GNSS+ Meeting*, (Denver, CO), 2022.

[3] J. E. Yoder and T. E. Humphreys, “Low-cost inertial aiding for deep-urban tightly-coupled multi-antenna precise GNSS,” *Navigation, Journal of the Institute of Navigation*, 2022. To be published.

[4] Z. Clements, J. E. Yoder, and T. E. Humphreys, “Carrier-phase and IMU based GNSS spoofing detection for ground vehicles,” in *Proceedings of the ION International Technical Meeting*, (Long Beach, CA), 2022.

[5] R. Tenny and T. E. Humphreys, “Robust navigation for urban air mobility via tight coupling of GNSS with terrestrial radionavigation and inertial sensing,” in *Proceedings of the ION GNSS+ Meeting*, (Denver, CO), 2022.

[6] R. X. Kor, P. A. Iannucci, and T. E. Humphreys, “Autonomous signal-situational awareness in a terrestrial radionavigation system,” in *2021 International Conference on Intelligent Transportation Systems (ITSC)*, IEEE, 2021.

[7] R. X. Kor, P. A. Iannucci, L. Narula, and T. E. Humphreys, “A proposal for securing terrestrial radionavigation systems,” in *Proceedings of the ION GNSS+ Meeting*, (Online), 2020.

[8] A. M. Graff, W. N. Blount, P. A. Iannucci, J. G. Andrews, and T. E. Humphreys, “Analysis of OFDM signals for ranging and communications,” in *Proceedings of the ION GNSS+ Meeting*, (St. Louis, MO), 2021.

[9] P. A. Iannucci and T. E. Humphreys, “Fused low-Earth-orbit GNSS,” *IEEE Transactions on Aerospace and Electronic Systems*, pp. 1–1, 2022.

[10] D. M. LaChapelle, L. Narula, and T. E. Humphreys, “Orbital war driving: Assessing transient GPS interference from LEO,” in *Proceedings of the ION GNSS+ Meeting*, (St. Louis, MO), 2021.

[11] Z. Clements, P. Ellis, M. L. Psiaki, and T. E. Humphreys, “Geolocation of terrestrial GNSS spoofing signals from low earth orbit,” in *Proceedings of the ION GNSS+ Meeting*, (Denver, CO), 2022.

[12] V. Passaro, A. Cuccovillo, L. Vaiani, M. De Carlo, and C. Campanella, “Gyroscope technology and applications: A review in the industrial perspective,” *Sensors*, vol. 17, no. 10, 2017.

[13] N. El-Sheimy and A. Youssef, “Inertial sensors technologies for navigation applications: state of the art and future trends,” *Satellite Navigation*, vol. 1:2, 2020.

[14] P. Groves, “Navigation using inertial sensors [tutorial],” *IEEE Aerospace and Electronic Systems Magazine*, vol. 30, no. 2, pp. 42–69, 2015.

[15] A. Noureldin, T. Karamat, and J. Georgy, *Fundamentals of Inertial Navigation, Satellite-based Positioning and their Integration*. Heidelberg, New York, Dordrecht, London: Springer, 1993.

[16] C. Jekeli, *Inertial Navigation Systems with Geodetic Applications*. Berlin, New York: Walter de Gruyter, 2001.

[17] Y. Yi, *On Improving the Accuracy and Reliability of GPS/IMU-Based Direct Sensor Georeferencing*. phdthesis, 2007.

[18] D. M. Akos and M. S. Braasch, “A software radio approach to global navigation satellite system receiver design,” in *Proceedings of the 52rd Annual Meeting of The Institute of Navigation*, (Cambridge, MA), pp. 455–463, 1996.

[19] D. M. Akos, P. Normark, P. Enge, A. Hansson, and A. Rosenlind, “Real-time GPS software radio receiver,” in *Proceedings of the ION National Technical Meeting*, (Long Beach, CA), pp. 809–816, Institute of Navigation, Jan. 2001.

[20] B. M. Ledvina, M. L. Psiaki, D. Sheinfeld, A. P. Cerruti, S. P. Powell, and P. M. Kintner, “A real-time GPS civilian L1/L2 software receiver,” in *Proc. of the Institute of Navigation GNSS*, pp. 21–24, 2004.

[21] Trimble, “Trimble catalyst,” June 2022. https://geospatial.trimble.com/products-and-solutions/trimble-catalyst.

[22] B. M. Ledvina, M. L. Psiaki, S. P. Powell, and P. M. Kintner, Jr., “Bit-wise parallel algorithms for efficient software correlation applied to a GPS software receiver,” *IEEE Transactions on Wireless Communications*, vol. 3, Sept. 2004.

[23] T. E. Humphreys, J. Bhatti, T. Pany, B. Ledvina, and B. O’Hanlon, “Exploiting multicore technology in software-defined GNSS receivers,” in *Proceedings of the ION GNSS Meeting*, (Savannah, GA), pp. 326–338, Institute of Navigation, 2009.

[24] J. T. Curran, C. Fernández-Prades, A. Morrison, and M. Bavaro, “The continued evolution of software-defined radio for GNSS,” *GPS World*, vol. 29, pp. 43–49, 2018.

[25] S. Gunawardena, T. Pany, and J. Curran, “ION GNSS software-defined radio metadata standard,” *Navigation, Journal of the Institute of Navigation*, vol. 68, no. 1, pp. 11–20, 2021.

[26] G. Heinrichs, M. Restle, C. Dreischer, and T. Pany, “NavX-NSR–a novel Galileo/GPS navigation software receiver,” in *Proc. ION GNSS 2007*, (Fort Worth,Texas), Institute of Navigation, Sept. 2007.

[27] T. Pany, T. Kraus, A. Schütz, M. Arizabaleta, D. Dötterböck, and J. Damph, “Recent enhancments of the multi-sensor navigation analysis tool (musnat),” in *Proceedings of the 34nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)*, 2021.

[28] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, and P. M. Kintner, Jr., “GNSS receiver implementation on a DSP: Status, challenges, and prospects,” in *Proceedings of the ION GNSS Meeting*, (Fort Worth, TX), pp. 2370–2382, Institute of Navigation, 2006.

[29] E. G. Lightsey, T. E. Humphreys, J. A. Bhatti, A. J. Joplin, B. W. O’Hanlon, and S. P. Powell, “Demonstration of a space capable miniature dual frequency GNSS receiver,” *Navigation*, vol. 61, pp. 53–64, Mar. 2014.

[30] T. E. Humphreys, M. J. Murrian, and L. Narula, “Deep-urban unaided precise global navigation satellite system vehicle positioning,” *IEEE Intelligent Transportation Systems Magazine*, vol. 12, no. 3, pp. 109–122, 2020.

[31] L. Narula, D. M. LaChapelle, M. J. Murrian, J. M. Wooten, T. E. Humphreys, J.-B. Lacambre, E. de Toldi, and G. Morvant, “TEX-CUP: The University of Texas Challenge for Urban Positioning,” in *Proceedings of the IEEE/ION PLANSx Meeting*, 2020.

[32] M. L. Psiaki, “Real-time generation of bit-wise parallel representations of over-sampled prn codes,” *IEEE Transactions on Wireless Communications*, vol. 5, pp. 487–491, March 2006.

[33] B. Ledvina, “Efficient real-time generation of bit-wise parallel representations of oversampled carrier replicas,” *Aerospace and Electronic Systems, IEEE Transactions on*, vol. 47, pp. 2921–2933, Oct. 2011.

[34] D. Borio and C. Gioia, “Gnss interference mitigation: A measurement and position domain assessment,” *NAVIGATION*, vol. 68, no. 1, pp. 93–114, 2021.

[35] T. Pany, D. Dötterböck, H. Gomez-Martinez, M. S. Hammed, F. Hörkner, T. Kraus, D. Maier, D. Sánchez-Morales, A. Schütz, P. Klima, *et al.*, “The multi-sensor navigation analysis tool (musnat)–architecture, lidar, gpu/cpu gnss signal processing,” in *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, pp. 4087–4115, 2019.

[36] J. B. Kenney, “Dedicated short-range communications (DSRC) standards in the United States,” *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[37] D. Fajardo, T.-C. Au, S. Waller, P. Stone, and D. Yang, “Automated intersection control: Performance of future innovation versus current traffic signal control,” *Transportation Research Record: Journal of the Transportation Research Board*, no. 2259, pp. 223–232, 2011.

[38] L. Narula, J. M. Wooten, M. J. Murrian, D. M. LaChapelle, and T. E. Humphreys, “Accurate collaborative globally-referenced digital mapping with standard GNSS,” *Sensors*, vol. 18, no. 8, 2018.

[39] M. Petovello, M. Cannon, and G. Lachapelle, “Benefits of using a tactical-grade IMU for high-accuracy positioning,” *Navigation, Journal of the Institute of Navigation*, vol. 51, no. 1, pp. 1–12, 2004.

[40] B. M. Scherzinger, “Precise robust positioning with inertially aided RTK,” *Navigation*, vol. 53, no. 2, pp. 73–83, 2006.

[41] H. T. Zhang, “Performance comparison on kinematic GPS integrated with different tactical-grade IMUs,” Master’s thesis, The University of Calgary, Jan. 2006.

[42] S. Kennedy, J. Hamilton, and H. Martell, “Architecture and system performance of SPAN—NovAtel’s GPS/INS solution,” in *Position, Location, And Navigation Symposium, 2006 IEEE/ION*, p. 266, IEEE, 2006.

[43] T. Li, H. Zhang, Z. Gao, Q. Chen, and X. Niu, “High-accuracy positioning in urban environments using single-frequency multi-GNSS RTK/MEMS-IMU integration,” *Remote Sensing*, vol. 10, no. 2, p. 205, 2018.

[44] S. Godha, “Performance evaluation of low cost MEMS-based IMU integrated with GPS for land vehicle navigation application,” Master’s thesis, The University of Calgary, 2006.

[45] P. J. Teunissen and A. Khodabandeh, “Review and principles of PPP-RTK methods,” *Journal of Geodesy*, vol. 89, no. 3, pp. 217–240, 2015.

[46] Y. Cui, X. Meng, Q. Chen, Y. Gao, C. Xu, S. Roberts, and Y. Wang, “Feasibility analysis of low-cost GNSS receivers for achieving required positioning performance in CAV applications,” in *2017 Forum on Cooperative Positioning and Service*, pp. 355–361, May 2017.

[47] D. P. Shepard and T. E. Humphreys, “High-precision globally-referenced position and attitude via a fusion of visual SLAM, carrier-phase-based GPS, and inertial measurements,” in *Proceedings of the IEEE/ION PLANS Meeting*, May 2014.

[48] K. M. Pesyna, Jr., *Advanced Techniques for Centimeter-Accurate GNSS Positioning on Low-Cost Mobile Platforms*. PhD thesis, The University of Texas at Austin, Dec. 2015.

[49] R. B. Ong, M. G. Petovello, and G. Lachapelle, “Assessment of GPS/GLONASS RTK under various operational conditions,” in *Proceedings of the ION GNSS Meeting*, pp. 3297–3308, 2009.

[50] J. Jackson, B. Davis, and D. Gebre-Egziabher, “An assessment of low-cost RTK GNSS receivers,” in *Proceedings of the IEEE/ION PLANSx Meeting*, (Monterey, CA), 2018.

[51] T. E. Humphreys, M. Murrian, and L. Narula, “Low-cost precise vehicular positioning in urban environments,” in *2018 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, pp. 456–471, April 2018.

[52] T. G. Reid, S. E. Houts, R. Cammarata, G. Mills, S. Agarwal, A. Vora, and G. Pandey, “Localization requirements for autonomous vehicles,” *SAE International Journal of Connected and Automated Vehicles*, vol. 2, no. 12-02-03-0012, pp. 173–190, 2019.

[53] L. Narula, P. A. Iannucci, and T. E. Humphreys, “All-weather sub-50-cm radar-inertial positioning,” *Field Robotics*, vol. 2, pp. 525–556, 2022.

[54] P. J. Teunissen and O. Montenbruck, eds., *Springer handbook of global navigation satellite systems*. Springer, 2017.

[55] M. Murrian, C. Gonzalez, T. E. Humphreys, and T. D. Novlan, “A dense reference network for mass-market centimeter-accurate positioning,” in *Proceedings of the IEEE/ION PLANS Meeting*, (Savannah, GA), 2016.

[56] D. Odijk, *Fast Precise GPS Positioning in the Presence of Ionospheric Delays*. No. no. 52 in Fast precise GPS positioning in the presence of ionospheric delays, NCG, Nederlandse Commissie voor Geodesie, 2002.

[57] M. Abd Rabbou and A. El-Rabbany, “Tightly coupled integration of GPS precise point positioning and MEMS-based inertial systems,” *GPS Solutions*, vol. 19, no. 4, pp. 601–609, 2015.

[58] Z. Gao, H. Zhang, M. Ge, X. Niu, W. Shen, J. Wickert, and H. Schuh, “Tightly coupled integration of multi-GNSS PPP and MEMS inertial measurement unit data,” *GPS Solutions*, vol. 21, no. 2, pp. 377–391, 2017.

[59] S. Vana, “Low-cost, triple-frequency multi-GNSS PPP and MEMS IMU integration for continuous navigation in urban environments,” in *Proceedings of the ION GNSS+ Meeting*, pp. 3234–3249, 2021.

[60] A. Elmezayen and A. El-Rabbany, “Ultra-low-cost tightly coupled triple-constellation GNSS PPP/MEMS-based INS integration for land vehicular applications,” *Geomatics*, vol. 1, no. 2, pp. 258–286, 2021.

[61] K. Nagai, M. Spenko, R. Henderson, and B. Pervan, “Evaluating INS/GNSS availability for self-driving cars in urban environments,” in *Proceedings of the ION International Technical Meeting*, pp. 243–253, 2021.

[62] Z. Yang, Z. Li, Z. Liu, C. Wang, Y. Sun, and K. Shao, “Improved robust and adaptive filter based on non-holonomic constraints for RTK/INS integrated navigation,” *Measurement Science and Technology*, 2021.

[63] S. Hong, M. H. Lee, H.-H. Chun, S.-H. Kwon, and J. L. Speyer, “Observability of error states in GPS/INS integration,” *IEEE Transactions on Vehicular Technology*, vol. 54, no. 2, pp. 731–743, 2005.

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

[65] M. L. Psiaki, B. W. O’Hanlon, S. P. Powell, J. A. Bhatti, K. D. Wesson, T. E. Humphreys, and A. Schofield, “GNSS spoofing detection using two-antenna differential carrier phase,” in *Proceedings of the ION GNSS+ Meeting*, (Tampa, FL), Institute of Navigation, 2014.

[66] P. J. Teunissen, “The LAMBDA method for the GNSS compass,” *Artificial Satellites*, vol. 41, no. 3, pp. 89–103, 2006.

[67] G. Giorgi and P. J. Teunissen, “Carrier phase GNSS attitude determination with the multivariate constrained LAMBDA method,” in *2010 IEEE Aerospace Conference*, pp. 1–12, IEEE, 2010.

[68] S. Wu, X. Zhao, C. Pang, L. Zhang, Z. Xu, and K. Zou, “Improving ambiguity resolution success rate in the joint solution of GNSS-based attitude determination and relative positioning with multivariate constraints,” *GPS Solutions*, vol. 24, no. 1, pp. 1–14, 2020.

[69] P. Henkel and C. Günther, “Reliable integer ambiguity resolution: multi-frequency code carrier linear combinations and statistical a priori knowledge of attitude,” *Navigation, Journal of the Institute of Navigation*, vol. 59, no. 1, pp. 61–75, 2012.

[70] P. Fan, W. Li, X. Cui, and M. Lu, “Precise and robust RTK-GNSS positioning in urban environments with dual-antenna configuration,” *Sensors*, vol. 19, no. 16, p. 3586, 2019.

[71] R. Hirokawa and T. Ebinuma, “A low-cost tightly coupled GPS/INS for small uavs augmented with multiple GPS antennas,” *Navigation, Journal of the Institute of Navigation*, vol. 56, no. 1, pp. 35–44, 2009.

[72] P. Henkel, A. Sperl, U. Mittmann, T. Fritzel, R. Strauss, and H. Steiner, "Precise 6D RTK positioning system for UAV-based near-field antenna measurements," in *2020 14th European Conference on Antennas and Propagation (EuCAP)*, pp. 1–5, IEEE, 2020.

[73] J. E. Yoder, P. A. Iannucci, L. Narula, and T. E. Humphreys, "Multi-antenna vision-and-inertial-aided CDGNSS for micro aerial vehicle pose estimation," in *Proceedings of the ION GNSS+ Meeting*, (Online), pp. 2281–2298, 2020.

[74] T. E. Humphreys, R. X. T. Kor, and P. A. Iannucci, "Open-world virtual reality headset tracking," in *Proceedings of the ION GNSS+ Meeting*, (Online), 2020.

[75] John A. Volpe National Transportation Systems Center, "Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System," 2001.

[76] M. L. Psiaki and T. E. Humphreys, *Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications*, vol. 1, ch. Civilian GNSS Spoofing, Detection, and Recovery, pp. 655–680. Wiley-IEEE, 2020.

[77] R. Mit, Y. Zangvil, and D. Katalan, "Analyzing tesla's level 2 autonomous driving system under different gnss spoofing scenarios and implementing connected services for authentication and reliability of gnss data," in *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, pp. 621–646, 2020.

[78] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.

[79] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS signal authentication via power and distortion monitoring," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, pp. 739–754, April 2018.

[80] J. N. Gross, C. Kilic, and T. E. Humphreys, "Maximum-likelihood power-distortion monitoring for GNSS-signal authentication," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 1, pp. 469–475, 2018.

[81] T. E. Humphreys, "Interference," in *Springer Handbook of Global Navigation Satellite Systems*, pp. 469–503, Springer International Publishing, 2017.

[82] P. Y. Montgomergy, T. E. Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," in *Proceedings of the ION International Technical Meeting*, (Anaheim, CA), Jan. 2009.

[83] H. Ye, Y. Chen, and M. Liu, "Tightly coupled 3d lidar inertial odometry and mapping," in *2019 International Conference on Robotics and Automation (ICRA)*, pp. 3144–3150, IEEE, 2019.

[84] K.-W. Chiang, G.-J. Tsai, Y.-H. Li, Y. Li, and N. El-Sheimy, "Navigation engine design for automated driving using INS/GNSS/3D LiDAR-SLAM and integrity assessment," *Remote Sensing*, vol. 12, no. 10, p. 1564, 2020.

[85] P. J. Teunissen, *Springer Handbook of Global Navigation Satellite Systems*, ch. Carrier Phase Integer Ambiguity Resolution, pp. 661–685. Springer, 2017.

[86] Center for International Earth Science Information Network - Columbia University, "Gridded Population of the World, Version 4 (GPWv4): Population Count, Revision 11," 2018.

[87] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR," in *Black Hat Europe*, 2015.

[88] C. Yan, W. Xu, and J. Liu, "Can You Trust Autonomous Vehicles: Contactless Attacks Against Sensors of Self-driving Vehicle," in *DEF CON*, 2016.

[89] S.-T. Chen, C. Cornelius, J. Martin, and D. H. P. Chau, "Shapeshifter: Robust Physical Adversarial Attack on Faster R-CNN Object Detector," in *Joint European Conference on Machine Learning and Knowledge Discovery in Databases (ECML PKDD)*, pp. 52–68, Springer, 2018.

[90] K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C. Xiao, A. Prakash, T. Kohno, and D. Song, “Robust Physical-World Attacks on Deep Learning Visual Classification,” in *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2018.

[91] K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, F. Tramer, A. Prakash, T. Kohno, and D. Song, “Physical Adversarial Examples for Object Detectors,” in *USENIX Workshop on Offensive Technologies (WOOT)*, 2018.

[92] Y. Zhao, H. Zhu, R. Liang, Q. Shen, S. Zhang, and K. Chen, “Seeing isn’t Believing: Practical Adversarial Attack Against Object Detectors,” in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2019.

[93] W. Jia, Z. Lu, H. Zhang, Z. Liu, J. Wang, and G. Qu, “Fooling the Eyes of Autonomous Vehicles: Robust Physical Adversarial Examples Against Traffic Sign Recognition Systems,” in *ISOC Network and Distributed System Security Symposium (NDSS)*, 2022.

[94] Y. Jia, Y. Lu, J. Shen, Q. A. Chen, H. Chen, Z. Zhong, and T. Wei, “Fooling Detection Alone is Not Enough: Adversarial Attack against Multiple Object Tracking,” in *International Conference on Learning Representations (ICLR)*, 2020.

[95] T. Sato, J. Shen, N. Wang, Y. J. Jia, X. Lin, and Q. A. Chen, “Dirty Road Can Attack: Security of Deep Learning based Automated Lane Centering under Physical-World Attack,” in *Usenix Security Symposium*, 2021.

[96] P. Jing, Q. Tang, Y. Du, L. Xue, X. Luo, T. Wang, S. Nie, and S. Wu, “Too Good to Be Safe: Tricking Lane Detection in Autonomous Driving with Crafted Perturbations,” in *Usenix Security Symposium*, 2021.

[97] T. Sato and Q. A. Chen, “Towards Driving-Oriented Metric for Lane Detection Models,” in *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2022.

[98] Y. Cao, N. Wang, C. Xiao, D. Yang, J. Fang, R. Yang, Q. A. Chen, M. Liu, and B. Li, “Invisible in both Camera and LiDAR: Security of Multi-Sensor Fusion based Perception in Autonomous Driving Under Physical-World Attacks,” in *IEEE Symposium on Security and Privacy (S&P)*, 2021.

[99] J. Wang, A. Liu, Z. Yin, S. Liu, S. Tang, and X. Liu, “Dual Attention Suppression Attack: Generate Adversarial Camouflage in Physical World,” in *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2021.

[100] K. Xu, G. Zhang, S. Liu, Q. Fan, M. Sun, H. Chen, P.-Y. Chen, Y. Wang, and X. Lin, “Adversarial T-shirt! Evading Person Detectors in A Physical World,” in *European Conference on Computer Vision (ECCV)*, pp. 665–681, Springer, 2020.

[101] Z. Wu, S.-N. Lim, L. S. Davis, and T. Goldstein, “Making an Invisibility Cloak: Real World Adversarial Attacks on Object Detectors,” in *European Conference on Computer Vision (ECCV)*, 2020.

[102] B. Nassi, Y. Mirsky, D. Nassi, R. Ben-Netanel, O. Drokin, and Y. Elovici, “Phantom of the ADAS: Securing Advanced Driver-Assistance Systems from Split-Second Phantom Attacks,” in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pp. 293–308, 2020.

[103] G. Lovisotto, H. Turner, I. Sluganovic, M. Strohmeier, and I. Martinovic, “SLAP: Improving Physical Adversarial Examples with Short-Lived Adversarial Perturbations,” in *USENIX Security Symposium*, 2021.

[104] K. Tang, J. Shen, and Q. A. Chen, “Fooling Perception via Location: A Case of Region-of-Interest Attacks on Traffic Light Detection in Autonomous Driving,” in *AutoSec Workshop at NDSS*, 2021.

[105] C. Yan, Z. Xu, Z. Yin, X. Ji, and W. Xu, “Rolling Colors: Adversarial Laser Exploits against Traffic Light Recognition,” in *USENIX Security Symposium*, 2022.

[106] W. Wang, Y. Yao, X. Liu, X. Li, P. Hao, and T. Zhu, “I Can See the Light: Attacks on Autonomous Vehicles Using Invisible Lights,” in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2021.

[107] Y. Man, M. Li, and R. Gerdes, “GhostImage: Remote Perception Attacks against Camera-based Image Classification Systems,” in *International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, 2020.

[108] S. Jung, S. Song, S. Kim, J. Park, J. Her, K. Roh, and H. Myung, “Toward autonomous bridge inspection: A framework and experimental results,” in *2019 16th International Conference on Ubiquitous Robots (UR)*, pp. 208–211, IEEE, 2019.

[109] T. Bilis, T. Kouimtzoglou, M. Magnisali, and P. Tokmakidis, “The use of 3D scanning and photogrammetry techniques in the case study of the roman theatre of nikopolis. surveying, virtual reconstruction and restoration study.,” *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. 42, no. 2/W3, 2017.

[110] J. Qi, D. Song, H. Shang, N. Wang, C. Hua, C. Wu, X. Qi, and J. Han, “Search and rescue rotary-wing UAV and its application to the Lushan MS 7.0 earthquake,” *Journal of Field Robotics*, vol. 33, no. 3, pp. 290–321, 2016.

[111] M. Psiaki and S. Mohiuddin, “Global positioning system integer ambiguity resolution using factorized least-squares techniques,” *Journal of Guidance, Control, and Dynamics*, vol. 30, pp. 346–356, March-April 2007.

[112] S. Verhagen, P. J. Teunissen, and D. Odijk, “The future of single-frequency integer ambiguity resolution,” in *VII Hotine-Marussi Symposium on Mathematical Geodesy*, pp. 33–38, Springer, 2012.

[113] F. Zimmermann, C. Eling, L. Klingbeil, and H. Kuhlmann, “Precise positioning of UAVs-dealing with challenging RTK-GPS measurement conditions during automated UAV flights.,” *ISPRS Annals of Photogrammetry, Remote Sensing & Spatial Information Sciences*, vol. 4, 2017.

[114] S. Godha, G. Lachapelle, and M. Cannon, “Integrated GPS/INS system for pedestrian navigation in a signal degraded environment,” in *Proceedings of the ION GNSS Meeting*, vol. 2006, 2006.

[115] A. Angrisano, M. Petovello, and G. Pugliano, “Benefits of combined GPS/GLONASS with low-cost MEMS IMUs for vehicular urban navigation,” *Sensors*, vol. 12, no. 4, pp. 5134–5158, 2012.

[116] J. Kelly and G. S. Sukhatme, “Visual-inertial sensor fusion: Localization, mapping and sensor-to-sensor self-calibration,” *The International Journal of Robotics Research*, vol. 30, no. 1, pp. 56–79, 2011.

[117] G. Huang, “Visual-inertial navigation: A concise review,” in *2019 International Conference on Robotics and Automation (ICRA)*, pp. 9572–9582, IEEE, 2019.

[118] M. Bloesch, M. Burri, S. Omari, M. Hutter, and R. Siegwart, “Iterated extended Kalman filter based visual-inertial odometry using direct photometric feedback,” *The International Journal of Robotics Research*, vol. 36, no. 10, pp. 1053–1072, 2017.

[119] A. I. Mourikis and S. I. Roumeliotis, “A multi-state constraint Kalman filter for vision-aided inertial navigation,” in *Proceedings 2007 IEEE International Conference on Robotics and Automation*, pp. 3565–3572, IEEE, 2007.

[120] M. Li and A. I. Mourikis, “High-precision, consistent EKF-based visual-inertial odometry,” *The International Journal of Robotics Research*, vol. 32, no. 6, pp. 690–711, 2013.

[121] Z. Huai and G. Huang, “Robocentric visual-inertial odometry,” in *2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pp. 6319–6326, IEEE, 2018.

[122] P. Henkel, A. Blum, and C. Günther, “Precise RTK positioning with GNSS, INS, barometer and vision,” in *Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2017)*, pp. 2290–2303, 2017.

[123] T. Li, H. Zhang, Z. Gao, X. Niu, and N. El-Sheimy, “Tight fusion of a monocular camera, MEMS-IMU, and single-frequency multi-GNSS RTK for precise navigation in GNSS-challenged environments,” *Remote Sensing*, vol. 11, no. 6, p. 610, 2019.

[124] P. Henkel, A. Sperl, U. Mittmann, R. Bensch, P. Färber, and C. Günther, “Precise positioning of robots with fusion of GNSS, INS, odometry, barometer, local positioning system and visual localization,” in *Proc. of the 31st Intern. Technical Meeting of The Satellite Division of the Institute of Navigation*, pp. 3078–3087, 2018.

[125] Z. Sun, S. Balakrishnan, L. Su, A. Bhuyan, P. Wang, and C. Qiao, “Who is in control? practical physical layer attack and defense for mmwave-based sensing in autonomous vehicles,” *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3199–3214, 2021.

[126] J. Choi, V. Va, N. Gonzalez-Prelcic, R. Daniels, C. R. Bhat, and R. W. Heath, “Millimeter-wave vehicular communication to support massive automotive sensing,” *IEEE Communications Magazine*, vol. 54, pp. 160–167, Dec. 2016.

[127] D. LaChapelle, T. E. Humphreys, L. Narula, P. A. Iannucci, and E. Moradi-Pari, “Automotive collision risk estimation under cooperative sensing,” in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, (Barcelona, Spain), 2020.

[128] H. Shin, D. Kim, Y. Kwon, and Y. Kim, “Illusion and Dazzle: Adversarial Optical Channel Exploits Against Lidars for Automotive Applications,” in *International Conference on Cryptographic Hardware and Embedded Systems (CHES)*, 2017.

[129] Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu, and Z. M. Mao, “Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving,” in *ACM Conference on Computer and Communications Security (CCS)*, 2019.

[130] J. Sun, Y. Cao, Q. A. Chen, and Z. M. Mao, “Towards Robust LiDAR-based Perception in Autonomous Driving: General Black-box Adversarial Sensor Attack and Countermeasures,” in *Usenix Security Symposium*, 2020.

[131] R. S. Hallyburton, Y. Liu, Y. Cao, Z. M. Mao, and M. Pajic, “Security Analysis of Camera-LiDAR Fusion against Black-Box Attacks on Autonomous Vehicles,” in *USENIX Security Symposium*, 2022.

[132] Y. Cao, S. H. Bhupathiraju, P. Naghavi, T. Sugawara, Z. M. Mao, and S. Rampazzi, “You Can’t See Me: Physical Removal Attacks on LiDAR-based Autonomous Vehicles Driving Frameworks,” in *USENIX Security Symposium*, 2023.

[133] K. Yang, T. Tsai, H. Yu, M. Panoff, T.-Y. Ho, and Y. Jin, “Robust Roadside Physical Adversarial Attack Against Deep Learning in Lidar Perception Modules,” in *ACM Asia Conference on Computer and Communications Security (AsiaCCS)*, pp. 349–362, 2021.

[134] Y. Zhu, C. Miao, T. Zheng, F. Hajiaghajani, L. Su, and C. Qiao, “Can We Use Arbitrary Objects to Attack LiDAR Perception in Autonomous Driving?,” in *PACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2021.

[135] Y. Zhu, C. Miao, F. Hajiaghajani, M. Huai, L. Su, and C. Qiao, “Adversarial Attacks against LiDAR Semantic Segmentation in Autonomous Driving,” in *ACM Conference on Embedded Networked Sensor Systems (SenSys)*, 2021.

[136] C. Rizos, G. Roberts, J. Barnes, and N. Gambale, “Experimental results of Locata: A high accuracy indoor positioning system,” in *2010 International Conference on Indoor Positioning and Indoor Navigation*, pp. 1–7, IEEE, 2010.

[137] S. Meiyappan, A. Raghupathy, and G. Pattabiraman, “Positioning in GPS challenged locations-the NextNav terrestrial positioning constellation,” *Proc. ION GNSS+ 2013*, 2013.

[138] C. Rizos, D. A. Grejner-Brzezinska, C. K. Toth, A. G. Dempster, Y. Li, N. Politi, J. Barnes, and H. Sun, “A hybrid system for navigation in GPS-challenged environments: Case study,” *Proceedings, ION GNSS, Savannah, Georgia, Sept*, pp. 16–19, 2008.

[139] C. Rizos and L. Yang, “Background and recent advances in the locata terrestrial positioning and timing technology,” *Sensors*, vol. 19, no. 8, p. 1821, 2019.

[140] J. Barnes, C. Rizos, M. Kanli, D. Small, G. Voigt, N. Gambale, J. Lamance, T. Nunan, and C. Reid, "Indoor industrial machine guidance using Locata: A pilot study at BlueScope Steel," in *60th Annual Meeting of the US Inst. Of Navigation*, pp. 533–540, 2004.

[141] F. A. Khan, C. Rizos, and A. G. Dempster, "Novel time-sharing scheme for virtual elimination of locata-WiFi interference effects," in *Int. Symp. on GPS/GNSS*, pp. 526–530, 2008.

[142] F. A. Khan, C. Rizos, and A. G. Dempster, "Locata performance evaluation in the presence of wide- and narrow-band interference," *Journal of Navigation*, vol. 63, no. 3, p. 527, 2010.

[143] L. Scott, "Anti-spoofing and authenticated signal architectures for civil navigation systems," in *Proceedings of the ION GNSS Meeting*, pp. 1542–1552, 2003.

[144] J. M. Anderson, K. L. Carroll, N. P. DeVilbiss, J. T. Gillis, J. C. Hinks, B. W. O'Hanlon, J. J. Rushanan, L. Scott, and R. A. Yazdi, "Chips-message robust authentication (Chimera) for GPS civilian signals," in *ION GNSS*, pp. 2388–2416, 2017.

[145] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proceedings of the ION GNSS Meeting*, (Savannah, GA), Institute of Navigation, 2008.

[146] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[147] J. Bhatti and T. E. Humphreys, "Hostile control of ships via false GPS signals: Demonstration and detection," *Navigation*, vol. 64, no. 1, pp. 51–66, 2017.

[148] M. L. Psiaki, B. W. O'Hanlon, S. P. Powell, J. A. Bhatti, T. E. Humphreys, and A. Schofield, "GNSS lies, GNSS truth: Spoofing detection with two-antenna differential carrier phase," *GPS World*, vol. 25, pp. 36–44, Feb. 2014.

[149] C4ADS, "Above us only stars: Exposing GPS spoofing in Russia and Syria," April 2019. https://c4ads.org/reports.

[150] M. J. Murrian, L. Narula, and T. E. Humphreys, "Characterizing terrestrial GNSS interference from low earth orbit," in *Proceedings of the ION GNSS+ Meeting*, Institute of Navigation, Oct. 2019.

[151] M. Harris, "Ghost ships, crop circles, and soft gold: A GPS mystery in Shanghai," *MIT Technology Review*, 11 2019.

[152] B. Bergman, "AIS Ship Tracking Data Shows False Vessel Tracks Circling Above Point Reyes, Near San Francisco," 05 2020.

[153] T. E. Humphreys, "Lost in Space: How Secure Is the Future of Mobile Positioning?," 02 2016.

[154] C. Yang, A. Soloviev, M. Veth, and D. Qiu, "Opportunistic Use of Metropolitan RF Beacon Signals for Urban and Indoor Positioning," in *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016), Portland, Oregon*, pp. 394–403, 2016.

[155] M. Meurer, A. Konovaltsev, M. Cuntz, and C. Hättich, "Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM," in *Proceedings of the 25th Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2012)*, ION, 2012.

[156] D. Borio, "PANOVA tests and their application to GNSS spoofing detection," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, pp. 381–394, Jan. 2013.

[157] L. He, H. Li, and M. Lu, "Dual-antenna GNSS spoofing detection method based on Doppler frequency difference of arrival," *GPS Solutions*, vol. 23, no. 3, p. 78, 2019.

[158] M. Psiaki, S. P. Powell, and B. W. O'Hanlon, "GNSS spoofing detection using high-frequency antenna motion and carrier-phase data," in *Proceedings of the ION GNSS+ Meeting*, pp. 2949–2991, 2013.

[159] A. Broumandan, A. Jafarnia-Jahromi, V. Dehgahanian, J. Nielsen, and G. Lachapelle, “GNSS spoofing detection in handheld receivers based on signal spatial correlation,” in *Proceedings of the IEEE/ION PLANS Meeting*, (Myrtle Beach, SC), Institute of Navigation, April 2012.

[160] E. McMilin, D. S. De Lorenzo, T. Walter, T. H. Lee, and P. Enge, “Single antenna GPS spoof detection that is simple, static, instantaneous and backwards compatible for aerial applications,” in *Proceedings of the 27th international technical meeting of the satellite division of the institute of navigation (ION GNSS+ 2014), Tampa, FL*, pp. 2233–2242, Citeseer, 2014.

[161] J.-P. Poncelet and D. M. Akos, “A low-cost monitoring station for detection & localization of interference in GPS L1 band,” in *2012 6th ESA Workshop on Satellite Navigation Technologies (Navitec 2012) & European Workshop on GNSS Signals and Signal Processing*, pp. 1–6, IEEE, 2012.

[162] Y. C. Lee and D. G. O’Laughlin, “Performance Analysis of a Tightly Coupled GPS/Inertial System for Two Integrity Monitoring Methods 1,” *Navigation*, vol. 47, no. 3, pp. 175–189, 2000.

[163] S. Khanafseh, N. Roshan, S. Langel, F.-C. Chan, M. Joerger, and B. Pervan, “GPS spoofing detection using RAIM with INS coupling,” in *Position, Location and Navigation Symposium-PLANS 2014, 2014 IEEE/ION*, pp. 1232–1239, IEEE, 2014.

[164] K. D. Wesson, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, “An evaluation of the vestigial signal defense for civil GPS anti-spoofing,” in *Proceedings of the ION GNSS Meeting*, (Portland, OR), 2011.

[165] C. Wullems, O. Pozzobon, and K. Kubik, “Signal authentication and integrity schemes for next generation global navigation satellite systems,” in *Proc. European Navigation Conference GNSS*, (Munich), July 2005.

[166] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, “A blueprint for civil GPS navigation message authentication,” in *Proceedings of the IEEE/ION PLANS Meeting*, May 2014.

[167] J. T. Curran and M. Paonni, “Securing GNSS: An end-to-end feasibility study for the Galileo open service,” in *International Technical Meeting of the Satellite Division of The Institute of Navigation, ION GNSS*, pp. 1–15, 2014.

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

[169] K. Chino, D. Manandhar, and R. Shibasaki, “Authentication technology using QZSS,” in *2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014*, pp. 367–372, IEEE, 2014.

[170] S. C. Lo and P. K. Enge, “Authenticating aviation augmentation system broadcasts,” in *IEEE/ION Position, Location and Navigation Symposium*, pp. 708–717, IEEE, 2010.

[171] A. Neish, T. Walter, and P. Enge, “Quantum-resistant authentication algorithms for satellite-based augmentation systems,” *Navigation*, vol. 66, no. 1, pp. 199–209, 2019.

[172] A. Neish, T. Walter, and J. D. Powell, “Design and analysis of a public key infrastructure for sbas data authentication,” *Navigation*, vol. 66, no. 4, pp. 831–844, 2019.

[173] P. Gutierrez, “Galileo to Transmit Open Service Authentication,” *Inside GNSS*, 2020.

[174] C. Hegarty, “Analytical model for GNSS receiver implementation losses,” *Navigation, Journal of the Institute of Navigation*, vol. 58, no. 1, p. 29, 2011.

[175] A. G. Dempster and E. Cetin, “Interference localization for satellite navigation systems,” *Proceedings of the IEEE*, vol. 104, pp. 1318–1326, June 2016.

[176] T. E. Humphreys, “Detection strategy for cryptographic GNSS anti-spoofing,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073–1090, 2013.

[177] C. Rocken and C. Meertens, “Monitoring selective availability dither frequencies and their effect on GPS data,” *Bulletin géodésique*, vol. 65, no. 3, pp. 162–169, 1991.

[178] P. Enge, “Local area augmentation of GPS for the precision approach of aircraft,” *Proceedings of the IEEE*, vol. 87, no. 1, pp. 111–132, 1999.

[179] G. N. Green and T. Humphreys, “Position-domain integrity analysis for generalized integer aperture bootstrapping,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 2, pp. 734–746, 2018.

[180] C. Torens, A. Volkert, D. Becker, D. Gerbeth, L. Schalk, O. Garcia Crespillo, C. Zhu, T. Stelkens-Kobsch, T. Gehrke, I. C. Metz, *et al.*, “HorizonUAM: Safety and security considerations for urban air mobility,” in *AIAA Aviation 2021 Forum*, p. 3199, 2021.

[181] C. Rizos, D. Grejner-Brzezinska, C. Toth, A. Dempster, Y. Li, N. Politi, J. Barnes, and H. Sun, “A hybrid system for navigation in GPS-challenged environments: Case study,” vol. 4, 08 2009.

[182] D. A. Grejner-Brzezinska, C. K. Toth, H. Sun, X. Wang, and C. Rizos, “A robust solution to high-accuracy geolocation: Quadruple integration of GPS, IMU, pseudolite, and terrestrial laser scanning,” *IEEE Transactions on Instrumentation and Measurement*, vol. 60, no. 11, pp. 3694–3708, 2011.

[183] W. Jiang, Y. Li, and C. Rizos, “Improved decentralized multi-sensor navigation system for airborne applications,” *GPS Solutions*, vol. 22, no. 78, 2018. https://doi.org/10.1007/s10291-018-0743-9.

[184] W. Jiang, Y. Li, C. Rizos, and J. Barnes, “Flight evaluation of a locata-augmented multisensor navigation system,” *Journal of Applied Geodesy*, vol. 7, 11 2013.

[185] W. Jiang, Y. Li, and C. Rizos, “Optimal data fusion algorithm for navigation using triple integration of ppp-gnss, ins, and terrestrial ranging system,” *IEEE Sensors Journal*, vol. 15, no. 10, pp. 5634–5644, 2015.

[186] A. Mohanty, A. Wu, S. Bhamidipati, and G. Gao, “Precise relative positioning via tight-coupling of GPS carrier phase and multiple UWBs,” *IEEE Robotics and Automation Letters*, pp. 1–1, 2022.

[187] M. Maaref, J. Khalife, and Z. M. Kassas, “Aerial vehicle protection level reduction by fusing gnss and terrestrial signals of opportunity,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 9, pp. 5976–5993, 2021.

[188] M. Jia, H. Lee, J. Khalife, Z. M. Kassas, and J. Seo, “Ground vehicle navigation integrity monitoring for multi-constellation gnss fused with cellular signals of opportunity,” in *2021 IEEE International Intelligent Transportation Systems Conference (ITSC)*, pp. 3978–3983, 2021.

[189] 3GPP, “Study on NR positioning support,” tr 38.901, 3rd Generation Partnership Project (3GPP), Mar. 2019. Version 16.0.0.

[190] R. Keating, M. Säily, J. Hulkkonen, and J. Karjalainen, “Overview of positioning in 5G new radio,” in *2019 16th International Symposium on Wireless Communication Systems (ISWCS)*, pp. 320–324, IEEE, 2019.

[191] S. Kalyani and K. Giridhar, “Mitigation of error propagation in decision directed OFDM channel tracking using generalized m estimators,” *IEEE Transactions on Signal Processing*, vol. 55, no. 5, pp. 1659–1672, 2007.

[192] K. Shi, E. Serpedin, and P. Ciblat, “Decision-directed fine synchronization in OFDM systems,” *IEEE Transactions on Communications*, vol. 53, no. 3, pp. 408–412, 2005.

[193] J. Ziv and M. Zakai, “Some lower bounds on signal parameter estimation,” *IEEE Transactions on Information Theory*, vol. 15, no. 3, pp. 386–391, 1969.

[194] P. Wang and Y. Morton, “Performance comparison of time-of-arrival estimation techniques for lte signals in realistic multipath propagation channels,” in *Proceedings of the ION GNSS+ Meeting*, pp. 2241–2253, Sept. 2019.

[195] J. A. del Peral-Rosado, J. A. López-Salcedo, F. Zanier, and G. Seco-Granados, “Position accuracy of joint time-delay and channel estimators in LTE networks,” *IEEE Access*, vol. 6, pp. 25185–25199, 2018.

[196] W. Xu, M. Huang, C. Zhu, and A. Dammann, “Maximum likelihood TOA and OTDOA estimation with first arriving path detection for 3GPP LTE system,” *Transactions on Emerging Telecommunications Technologies*, vol. 27, no. 3, pp. 339–356, 2016.

[197] D. Wang and M. Fattouche, “OFDM transmission for time-based range estimation,” *IEEE Signal Processing Letters*, vol. 17, pp. 571–574, June 2010.

[198] K. Shamaei, J. Khalife, and Z. M. Kassas, “Exploiting LTE signals for navigation: Theory to implementation,” *IEEE Transactions on Wireless Communications*, vol. 17, no. 4, pp. 2173–2189, 2018.

[199] M. L. Psiaki and B. D. Slosman, “Tracking of digital FM OFDM signals for the determination of navigation observables,” in *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, pp. 2325–2348, 2019.

[200] D. Serant, P. Thevenon, M. Boucheret, O. Julien, C. Macabiau, S. Corazza, M. Dervin, and L. Ries, “Development and validation of an OFDM/DVB-T sensor for positioning,” in *Proceedings of the IEEE/ION PLANS Meeting*, pp. 988–1001, IEEE/Institute of Navigation, 2010.

[201] M. Rabinowitz and J. Spilker, “A new positioning system using television synchronization signals,” *IEEE Transactions on Broadcasting*, vol. 51, no. 1, pp. 51–61, 2005.

[202] M. Driusso, M. Comisso, F. Babich, and C. Marshall, “Performance analysis of time of arrival estimation on OFDM signals,” *IEEE Signal Processing Letters*, vol. 22, no. 7, pp. 983–987, 2015.

[203] T. Wang, Y. Shen, and S. Mazuelas, “Bounds for OFDM ranging accuracy in multipath channels,” in *2011 IEEE International Conference on Ultra-Wideband (ICUWB)*, pp. 450–454, 2011.

[204] H. Dun, C. C. J. M. Tiberius, C. E. V. Diouf, and G. J. M. Janssen, “Design of sparse multiband signal for precise positioning with joint low-complexity time delay and carrier phase estimation,” *IEEE Transactions on Vehicular Technology*, vol. 70, no. 4, pp. 3552–3567, 2021.

[205] M. D. Larsen, G. Seco-Granados, and A. L. Swindlehurst, “Pilot optimization for time-delay and channel estimation in OFDM systems,” in *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 3564–3567, 2011.

[206] Y. Karisan, D. Dardari, S. Gezici, A. A. D’Amico, and U. Mengali, “Range estimation in multicarrier systems in the presence of interference: Performance limits and optimal signal design,” *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3321–3331, 2011.

[207] O. Üreten and S. Tascioundefinedlu, “Autocorrelation properties of OFDM timing synchronization waveforms employing pilot subcarriers,” *EURASIP Journal on Wireless Communications and Networking*, Jan. 2009.

[208] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[209] T. Yoo and A. Goldsmith, “Capacity of fading MIMO channels with channel estimation error,” in *2004 IEEE International Conference on Communications*, vol. 2, pp. 808–813, 2004.

[210] X. Tang, M. Alouini, and A. Goldsmith, “Effect of channel estimation error on m-qam ber performance in rayleigh fading,” *IEEE Transactions on Communications*, vol. 47, no. 12, pp. 1856–1864, 1999.

[211] S. Ohno and G. Giannakis, “Capacity maximizing mmse-optimal pilots for wireless ofdm over frequency-selective block rayleigh-fading channels,” *IEEE Transactions on Information Theory*, vol. 50, no. 9, pp. 2138–2145, 2004.

[212] Y. J. Morton, F. van Diggelen, J. J. Spilker Jr, B. W. Parkinson, S. Lo, and G. Gao, *Position, Navigation, and Timing Technologies in the 21st Century, Volumes 1 and 2: Integrated Satellite Navigation, Sensor Systems, and Civil Applications, Set*. John Wiley & Sons, 2020.

[213] J. J. Spilker, Jr., *Global Positioning System: Theory and Applications*, ch. 3: GPS Signal Structure and Theoretical Performance, pp. 57–119. Washington, D.C.: American Institute of Aeronautics and Astronautics, 1996.

[214] J. J. Spilker, Jr., *Global Positioning System: Theory and Applications*, ch. 20: Interference Effects and Mitigation Techniques, pp. 717–771. Washington, D.C.: American Institute of Aeronautics and Astronautics, 1996.

[215] E. C. Dolman, “New frontiers, old realities,” *Strategic Studies Quarterly*, vol. 6, no. 1, pp. 78–96, 2012.

[216] B. Gertz, “Air Force Gen. John W. Raymond: Chinese lasers, jammers threaten GPS satellites,” June 2021.

[217] O. Luba, L. Boyd, A. Gower, and J. Crum, “GPS III system operations concepts,” *IEEE Aerospace and Electronic Systems Magazine*, vol. 20, no. 1, pp. 10–18, 2005.

[218] T. E. Humphreys, L. Young, and T. Pany, “Considerations for future IGS receivers,” in *Position Paper of the 2008 IGS Workshop*, 2008.

[219] P. A. Iannucci and T. E. Humphreys, “Economical fused LEO GNSS,” in *Proceedings of the IEEE/ION PLANSx Meeting*, 2020.

[220] N. Levanon, “Quick position determination using 1 or 2 LEO satellites,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 34, no. 3, pp. 736–754, 1998.

[221] M. Rabinowitz, B. Parksinson, and J. Spilker, “Some capabilities of a joint GPS-LEO navigation system,” in *Proceedings of the 13th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2000)*, pp. 255–265, 2000.

[222] D. Lawrence, H. S. Cobb, G. Gutt, F. Tremblay, P. Laplante, and M. O’Connor, “Test results from a LEO-satellite-based assured time and location solution,” in *Proceedings of the 2016 International Technical Meeting of The Institute of Navigation*, pp. 125–129, 2016.

[223] J. J. Khalife and Z. M. Kassas, “Receiver design for Doppler positioning with LEO satellites,” in *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 5506–5510, 2019.

[224] J. Khalife, M. Neinavaie, and Z. M. Kassas, “Blind Doppler estimation from LEO satellite signals: A case study with real 5G signals,” in *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, pp. 3046–3054, 2020.

[225] Z. M. Kassas, *Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications*, vol. 1, ch. Navigation with Cellular Signals of Opportunity, pp. 1171–1224. Wiley-IEEE, 2020.

[226] Z. M. Kassas, *Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications*, vol. 1, ch. Navigation from Low Earth Orbit: Part 2: Models, Implementation, and performance, pp. 1381–1412. Wiley-IEEE, 2020.

[227] N. Levanon, “Theoretical bounds on random errors in satellite Doppler navigation,” *IEEE Transactions on Aerospace and Electronic Systems*, no. 6, pp. 810–816, 1984.

[228] D. Lawrence, H. Cobb, G. Gutt, M. OConnor, T. Reid, T. Walter, and D. Whelan, “Navigation from LEO: Current capability and future promise,” *GPS World*, vol. 28, no. 7, pp. 42–48, 2017.

[229] C. T. Ardito, J. J. Morales, J. Khalife, A. Abdallah, Z. M. Kassas, *et al.*, “Performance evaluation of navigation using LEO satellite signals with periodically transmitted satellite positions,” in *Proceedings of the 2019 International Technical Meeting of The Institute of Navigation*, pp. 306–318, 2019.

[230] H. Benzerrouk, Q. Nguyen, F. Xiaoxing, A. Amrhar, A. V. Nebylov, and R. Landry, “Alternative PNT based on Iridium Next LEO satellites Doppler/INS integrated navigation system,” in *2019 26th Saint Petersburg International Conference on Integrated Navigation Systems (ICINS)*, pp. 1–10, IEEE, 2019.

[231] T. G. R. Reid, A. M. Neish, T. Walter, and P. K. Enge, “Leveraging commercial broadband LEO constellations for navigation,” in *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, (Portland, Oregon), pp. 2300–2314, Sept. 2016.

[232] T. G. Reid, A. M. Neish, T. Walter, and P. K. Enge, “Broadband LEO constellations for navigation,” *Navigation, Journal of the Institute of Navigation*, vol. 65, no. 2, pp. 205–220, 2018.

[233] T. G. R. Reid, T. Walter, P. K. Enge, D. Lawrence, S. Cobb, G. Gutt, M. O’Connor, and D. Whelan, *Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications*, vol. 1, ch. Navigation from Low Earth Orbit: Part 1: Concept, Capability, and Future Promise., pp. 1359–1380. Wiley-IEEE, 2020.

[234] T. G. Reid, B. Chan, A. Goel, K. Gunning, B. Manning, J. Martin, A. Neish, A. Perkins, and P. Tarantino, “Satellite navigation for the age of autonomy,” in *Proceedings of the IEEE/ION PLANSx Meeting*, pp. 342–352, IEEE, 2020.

[235] Z. M. Kassas and T. E. Humphreys, “Receding horizon trajectory optimization in opportunistic navigation environments,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 51, pp. 866–877, April 2015.

[236] Z. M. Kassas, A. Arapostathis, and T. E. Humphreys, “Greedy motion planning for simultaneous signal landscape mapping and receiver localization,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, pp. 247 – 258, March 2015.

[237] J. J. Spilker, *Global Positioning System: Theory and Applications*, ch. 5: Satellite Constellation and Geometric Dilution of Precision, pp. 177–208. Washington, D.C.: American Institute of Aeronautics and Astronautics, 1996.

[238] M. L. Psiaki, “Navigation using carrier Doppler shift from a LEO constellation: TRANSIT on steroids,” *Navigation, Journal of the Institute of Navigation*, vol. 68, no. 3, pp. 621–641, 2021.

[239] B. McLemore and M. L. Psiaki, “Navigation using Doppler shift from LEO constellations and INS data,” in *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, pp. 3071–3086, 2020.

[240] SpaceX, “Revised SpaceX Gen2 non-geostationary satellite system, Technical Attachment.” https://licensing.fcc.gov/myibfs/download.do?attachment_key=12943362, Aug. 2021. SAT-AMD-20210818-00105.

[241] K. Systems, “Application for fixed satellite service by Kuiper Systems LLC.” https://licensing.fcc.gov/myibfs/download.do?attachment_key=1773885, July 2019. SAT-LOA-20190704-00057.

[242] M. Neinavaie, J. Khalife, and Z. M. Kassas, “Exploiting Starlink signals for navigation: First results,” in *Proceedings of the ION GNSS+ Meeting*, (St. Louis, Missouri), pp. 2766–2773, Sept. 2021.

[243] S. engineering team, “We are the Starlink team, ask us anything!,” Nov. 2020. https://www.reddit.com/r/Starlink/comments/jybmgn/we_are_the_starlink_team_ask_us_anything/.

[244] Space Exploration Holdings, “SpaceX Gen2 NGSO Satellite System, Attachment Waiver Requests.” https://licensing.fcc.gov/myibfs/download.do?attachment_key=2378667, May 2020. SAT-LOA-20200526-00055.

[245] SpaceX, “SpaceX non-geostationary satellite system, Technical Parameters.” https://licensing.fcc.gov/myibfs/download.do?attachment_key=1877844, Aug. 2019. SAT-MOD-20190830-00087.

[246] O. B. Osoro and E. J. Oughton, “A techno-economic framework for satellite networks applied to low earth orbit constellations: Assessing Starlink, OneWeb and Kuiper,” *IEEE Access*, vol. 9, pp. 141611–141625, 2021.

[247] Z. Liu, S. Lo, and T. Walter, “Gnss interference characterization and localization using opensky ads-b data,” *Multidisciplinary Digital Publishing Institute Proceedings*, vol. 59, no. 1, 2020.

[248] D. Goward, “Russia ramps up GPS jamming along with troops at ukraine border,” *GPS World*, Apr 2021.

[249] *Does radio frequency interference to satellite navigation pose an increasing threat to network efficiency, cost-effectiveness and ultimately safety?* Eurocontrol Aviation Intelligence Unit, Mar 2021.

[250] M. A. Garcia, J. Dolan, and A. Hoag, “Aireon’s initial on-orbit performance analysis of space-based ads-b,” in *2017 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, pp. 4A1–1–4A1–8, 2017.

[251] J. Stader and S. Gunawardena, “Leveraging worldwide, publicly-available data to create an automated satnav interference detection system,” in *Proceedings of the 2021 International Technical Meeting of The Institute of Navigation*, pp. 69–83, 2021.

[252] K. Sarda, D. CaJacob, N. Orr, and R. Zee, “Making the invisible visible: Precision rf-emitter geolocation from space by the hawkEye 360 pathfinder mission,” in *Proceedings of the 32nd Annual AIAA/USU Conference on Small Satellites,* Next on the Pad, no. SSC18-II-06, 2018.

[253] D. Werner, “First hawkeye 360 satellites pinpointing signals,” *SpaceNews*, Feb 2019.

[254] M. J. Murrian, L. Narula, P. A. Iannucci, S. Budzien, B. W. O’Hanlon, S. P. Powell, and T. E. Humphreys, “First results from three years of GNSS interference monitoring from low Earth orbit,” *Navigation, Journal of the Institute of Navigation*, vol. 68, no. 4, pp. 673–685, 2021.

[255] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection: a survey,” *ACM Computing Surveys*, vol. 41, no. 3, pp. 1–72, 2009.

[256] Y. Rajabzadeh, A. H. Rezaie, and H. Amindavar, “A dynamic modeling approach for anomaly detection using stochastic differential equations,” *Digital Signal Processing*, vol. 54, pp. 1–11, 2016.

[257] Z. Xu, K. Kersting, and L. Von Ritter, “Stochastic online anomaly analysis for streaming time series,” in *IJCAI*, pp. 3189–3195, 2017.

[258] D. Miralles, A. Bornot, P. Rouquette, N. Levigne, D. M. Akos, Y.-H. Chen, S. Lo, and T. Walter, “An assessment of gps spoofing detection via radio power and signal quality monitoring for aviation safety operations,” *IEEE Intelligent Transportation Systems Magazine*, vol. 12, no. 3, pp. 136–146, 2020.

[259] F. Bastide, E. Chatre, and C. Macabiau, “GPS interference detection and identification using multicorrelator receivers,” in *Proceedings of the 14th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2001)*, pp. 872–881, 2001.

[260] G. O’Mahony, S. O’Mahony, J. T. Curran, and C. C. Murphy, “Developing a low-cost platform for gnss interference detection,” in *Proceedings of the 2015 European Navigation Conference, Bordeaux, France*, 2015.

[261] A. Ndili and P. Enge, “Gps receiver autonomous interference detection,” in *IEEE 1998 Position Location and Navigation Symposium (Cat. No. 98CH36153)*, pp. 123–130, IEEE, 1996.

[262] E. G. Manfredini, D. M. Akos, Y.-H. Chen, S. Lo, T. Walter, and P. Enge, “Effective gps spoofing detection utilizing metrics from commercial receivers,” in *Proceedings of the 2018 International Technical Meeting of The Institute of Navigation*, pp. 672–689, 2018.

[263] S. Hewitson and J. Wang, “Gnss receiver autonomous integrity monitoring (raim) performance analysis,” *GPS Solutions*, vol. 10, no. 3, pp. 155–170, 2006.

[264] C. Hegarty, A. Odeh, K. Shallberg, K. Wesson, T. Walter, and K. Alexander, “Spoofing detection for airborne GNSS equipment,” in *Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018)*, pp. 1350–1368, 2018.

[265] H. V. Poor and O. Hadjiliadis, *Quickest detection*. Cambridge University Press, 2008.

[266] C. Truong, L. Oudre, and N. Vayatis, “Selective review of offline change point detection methods,” *Signal Processing*, vol. 167, p. 107299, 2020.

[267] D. A. Divis, “Scientists document possible drone jamming,” *Inside unmanned systems*, p. 14, Sept. 2015.

[268] M. J. Murrian, L. Narula, T. E. Humphreys, B. W. O’Hanlon, and S. Budzien, “Characterizing GNSS interference from low-earth orbit,” *Inside GNSS*, vol. 15, no. 1, pp. 54–59, 2020.

[269] K. Ho and Y. Chan, “Geolocation of a known altitude object from TDOA and FDOA measurements,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 33, pp. 770–783, July 1997.

[270] J. Bhatti, *Sensor Deception Detection and Radio-Frequency Emitter Localization*. PhD thesis, The University of Texas at Austin, Aug. 2015.

[271] A. Weiss, “Direct geolocation of wideband emitters based on delay and Doppler,” *Signal Processing, IEEE Transactions on*, vol. 59, pp. 2513–2521, June 2011.

[272] A. Sidi and A. Weiss, “Delay and Doppler induced direct tracking by particle filter,” *Aerospace and Electronic Systems, IEEE Transactions on*, vol. 50, pp. 559–572, January 2014.

[273] H. Witzgall, “Two-sensor tracking of maneuvering transmitters,” in *2018 IEEE Aerospace Conference*, pp. 1–7, IEEE, 2018.

[274] D. Musicki, R. Kaune, and W. Koch, “Mobile emitter geolocation and tracking using tdoa and fdoa measurements,” *Signal Processing, IEEE Transactions on*, vol. 58, pp. 1863–1874, March 2010.

[275] K. Ho and W. Xu, “An accurate algebraic solution for moving source location using tdoa and fdoa measurements,” *Signal Processing, IEEE Transactions on*, vol. 52, pp. 2453–2463, Sept 2004.

[276] K. Ho and Y. Chan, “Solution and performance analysis of geolocation by TDOA,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 29, no. 4, pp. 1311–1322, 1993.

[277] P. Ellis, D. V. Rheeden, and F. Dowla, “Use of Doppler and Doppler rate for RF geolocation using a single LEO satellite,” *IEEE Access*, vol. 8, pp. 12907–12920, 2020.

[278] K. Becker, “An efficient method of passive emitter location,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 28, no. 4, pp. 1091–1104, 1992.

[279] B. W. Parkinson, T. Stansell, R. Beard, and K. Gromov, “A history of satellite navigation,” *NAVIGATION: Journal of the Institute of Navigation*, vol. 42, no. 1, pp. 109–164, 1995.

[280] P. B. Ellis and F. Dowla, “Single satellite emitter geolocation in the presence of oscillator and ephemeris errors,” in *2020 IEEE Aerospace Conference*, pp. 1–7, IEEE, 2020.

[281] P. Ellis and F. Dowla, “Performance bounds of a single LEO satellite providing geolocation of an RF emitter,” in *2018 9th Advanced Satellite Multimedia Systems Conference and the 15th Signal Processing for Space Communications Workshop (ASMS/SPSC)*, pp. 1–5, IEEE, 2018.

[282] M. Ahrholdt, F. Bodereau, C. Fischer, M. Goppelt, R. Pietsch, A. John, A. Ossowska, and M. Kunert, “D12.1-study report on relevant scenarios and applications and requirements specification,” *European Commission: MOre Safety for All by Radar Interference Mitigation (MOSARIM)*, 2010.

[283] M. Kunert, F. Bodereau, M. Goppelt, C. Fischer, A. John, T. Wixforth, A. Ossowska, and T. S. et al., “D1.5-study on the state-of-the-art interference mitigation techniques,” *European Commission: MOre Safety for All by Radar Interference Mitigation (MOSARIM)*, 2010.

[284] S. Alland, W. Stark, M. Ali, and M. Hegde, “Interference in automotive radar systems: Characteristics, mitigation techniques, and current and future research,” *IEEE Signal Processing Magazine*, vol. 36, no. 5, pp. 45–59, 2019.

[285] R. Komissarov and A. Wool, “Spoofing attacks against vehicular fmcw radar,” in *Proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security*, pp. 91–97, 2021.

[286] N. Miura, T. Machida, K. Matsuda, M. Nagata, S. Nashimoto, and D. Suzuki, “A low-cost replica-based distance-spoofing attack on mmwave fmcw radar,” in *Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop*, pp. 95–100, 2019.

[287] P. Nallabolu and C. Li, “A frequency-domain spoofing attack on fmcw radars and its mitigation technique based on a hybrid-chirp waveform,” *IEEE Transactions on Microwave Theory and Techniques*, vol. 69, no. 11, pp. 5086–5098, 2021.

[288] M. Gardill, J. Schwendner, and J. Fuchs, “In-situ time-frequency analysis of the 77 ghz bands using a commercial chirp-sequence automotive fmcw radar sensor,” in *2019 IEEE MTT-S International Microwave Symposium (IMS)*, pp. 544–547, IEEE, 2019.

[289] M. Gardill, J. Schwendner, and J. Fuchs, “An approach to over-the-air synchronization of commercial chirp-sequence automotive radar sensors,” in *2020 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNeT)*, pp. 46–49, IEEE, 2020.

[290] S. Roehr, P. Gulden, and M. Vossiek, “Method for high precision clock synchronization in wireless systems with application to radio navigation,” in *2007 IEEE Radio and Wireless Symposium*, pp. 551–554, IEEE, 2007.

[291] T. Goddard, K. B. Kahn, and A. Adkins, “Racial bias in driver yielding behavior at crosswalks,” *Transportation research part F: traffic psychology and behaviour*, vol. 33, pp. 1–6, 2015. Publisher: Elsevier.

[292] A. J. Haddad, A. Mondal, C. R. Bhat, A. Zhang, M. C. Liao, L. J. Macias, M. K. Lee, and S. C. Watkins, “Pedestrian crash frequency: Unpacking the effects of contributing factors and racial disparities,” *Accident; Analysis and Prevention*, vol. 182, p. 106954, March 2023.

[293] V. John, S. Mita, Z. Liu, and B. Qi, “Pedestrian detection in thermal images using adaptive fuzzy C-means clustering and convolutional neural networks,” pp. 246–249, IEEE, 2015.

[294] K. A. Perrine, A. Haddad, L. Macias, and C. R. Bhat, “Synthesis of automated pedestrian data collection technologies,” Final research report FHWA/TX-22/0-7126-1, Texas Department of Transportation, 2022.

[295] B. Blanc, P. Johnson, M. Figliozzi, C. Monsere, and K. Nordback, “Leveraging signal infrastructure for nonmotorized counts in a statewide program: pilot study,” *Transportation research record*, vol. 2527, no. 1, pp. 69–79, 2015. Publisher: SAGE Publications Sage CA: Los Angeles, CA.

[296] U. Gawande, K. Hajari, and Y. Golhar, “Pedestrian detection and tracking in video surveillance system: issues, comprehensive review, and challenges,” *Recent Trends in Computational Intelligence*, 2020. Publisher: IntechOpen.

[297] L. Chen, I. Grimstead, D. Bell, J. Karanka, L. Dimond, P. James, L. Smith, and A. Edwardes, “Estimating vehicle and pedestrian activity from town and city traffic cameras,” *Sensors*, vol. 21, no. 13, p. 4564, 2021. Publisher: Multidisciplinary Digital Publishing Institute.

[298] P. Lin, A. Kourtellis, Z. Wang, and C. Chen, “Integration of a robust automated pedestrian detection system for signalized intersections,” 2019.

[299] L. Yu, Y. Wang, X. Sun, and S. Han, “Thermal imaging pedestrian detection algorithm based on attention guidance and local cross-level network,” *Journal of Electronic Imaging*, vol. 30, no. 5, 2021. Publisher: SPIE.

[300] N. Shah, C. Cherry, C. Brakewood, M. Cate, A. Kohls, M. Ortmann, and F. Proulx, “TDOT bicycle & pedestrian counting: Best methodologies assessment,” Tech. Rep. RES2019-13, University of Tennessee-Center for Transportation Research, 2020.

[301] S. Kothuri, K. Nordback, A. Schrope, T. Phillips, and M. Figliozzi, “Bicycle and pedestrian counts at signalized intersections using existing infrastructure: Opportunities and challenges,” *Transportation Research Record*, vol. 2644, no. 1, pp. 11–18, 2017. Publisher: SAGE Publications Sage CA: Los Angeles, CA.

[302] J. Zhao, H. Xu, H. Liu, J. Wu, Y. Zheng, and D. Wu, “Detection and tracking of pedestrians and vehicles using roadside LiDAR sensors,” *Transportation Research Part C: Emerging Technologies*, vol. 100, pp. 68–87, 2019. Publisher: Elsevier.

[303] K. Liu, W. Wang, and J. Wang, “Pedestrian detection with LiDAR point clouds based on single template matching,” *Electronics*, vol. 8, no. 7, p. 780, 2019. Publisher: Multidisciplinary Digital Publishing Institute.

[304] H. Liu, C. Wu, and H. Wang, “Real time object detection using LiDAR and camera fusion for autonomous driving,” *Scientific Reports*, vol. 13, no. 1, p. 8056, 2023. Publisher: Nature Publishing Group UK London.

[305] A. C. Plascencia, P. García-Gómez, E. B. Perez, G. DeMas-Giménez, J. R. Casas, and S. Royo, “A preliminary study of deep learning sensor fusion for pedestrian detection,” *Sensors*, vol. 23, no. 8, p. 4167, 2023. Publisher: MDPI.

[306] Y. Hu, A. Perrig, and D. B. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks,” in *IEEE International Conference on Computer Communications (INFOCOM)*, 2003.

[307] W. Whyte, J. Petit, V. Kumar, J. Moring, and R. Roy, “Threat and Countermeasures Analysis for WAVE Service Advertisement,” in *IEEE International Conference on Intelligent Transportation Systems (ITSC)*, 2015.

[308] C. Laurendeau and M. Barbeau, “Threats to Security in DSRC/WAVE,” in *Proc. ADHOC-NOW*, 2006.

[309] J. Petit and S. E. Shladover, “Potential cyberattacks on automated vehicles,” *IEEE Trans. Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2015.

[310] J. Bellardo and S. Savage, “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions,” in *USENIX Security Symposium*, 2003.

[311] S. Hu, Q. A. Chen, J. Sun, Y. Feng, Z. M. Mao, and H. X. Liu, “Automated Discovery of Denial-of-Service Vulnerabilities in Connected Vehicle Protocols,” in *USENIX Security Symposium*, 2021.

[312] M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, “Security Vulnerabilities of Connected Vehicle Streams and Their Impact on Cooperative Driving,” in *IEEE Communications Magazine*, 2015.

[313] A. Abdo, S. M. B. Malek, Z. Qian, Q. Zhu, M. Barth, and N. Abu-Ghazaleh, “Application Level Attacks on Connected Vehicle Protocols,” in *International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, 2019.

[314] S. Dadras, R. M. Gerdes, and R. Sharma, “Vehicular Platooning in an Adversarial Environment,” in *ACM Symposium on Information, Computer and Communications Security (AsiaCCS)*, 2015.

[315] Q. A. Chen, Y. Yin, Y. Feng, Z. M. Mao, and H. X. Liu, “Exposing Congestion Attack on Emerging Connected Vehicle based Traffic Signal Control,” in *ISOC Network and Distributed System Security Symposium (NDSS)*, 2018.

[316] Y. Feng, S. Huang, Q. A. Chen, H. X. Liu, and Z. M. Mao, “Vulnerability of Traffic Control System Under Cyber-Attacks Using Falsified Data,” in *Transportation Research Board 2018 Annual Meeting (TRB)*, 2018.

[317] Y. Feng, S. E. Huang, W. Wong, Q. A. Chen, Z. M. Mao, and H. X. Liu, “On the Cybersecurity of Traffic Signal Control System With Connected Vehicles,” *IEEE Transactions on Intelligent Transportation Systems (ITS)*, 2022.

[318] W. Wong, S. Huang, Y. Feng, Q. A. Chen, Z. M. Mao, and H. X. Liu, “Trajectory-Based Hierarchical Defense Model to Detect Cyber-Attacks on Transportation Infrastructure,” tech. rep., 2019.

[319] S. Hu, Q. A. Chen, J. Joung, C. Carlak, Y. Feng, Z. M. Mao, and H. X. Liu, “CVShield: Guarding Sensor Data in Connected Vehicle with Trusted Execution Environment,” in *ACM Workshop on Automotive and Aerial Vehicle Security (AutoSec)*, 2020.

[320] M. Raja and U. Guven, “Design of obstacle avoidance and waypoint navigation using global position sensor/ultrasonic sensor,” *INCAS Bulletin*, vol. 13, no. 1, pp. 149–158, 2021.

[321] S. Sood, J. S. Sodhi, P. Maheshwari, K. Uppal, and D. Chakravarty, “Multiple waypoint navigation in unknown indoor environments,” *arXiv preprint arXiv:2209.08663*, 2022.

[322] F. Nofandi, R. Devandra, S. Hasugian, I. Sutrisno, and E. Setiawan, “Design floating robot of shallots irrigation with gps based and using the waypoint navigation method,” in *IOP Conference Series: Materials Science and Engineering*, vol. 1175, p. 012006, IOP Publishing, 2021.

[323] P. Lin, W. Y. Choi, J. H. Yang, and C. C. Chung, “Waypoint tracking for collision avoidance using artificial potential field,” in *2020 39th Chinese Control Conference (CCC)*, pp. 5455–5460, IEEE, 2020.

[324] P. Lin, W. Y. Choi, and C. C. Chung, “Local path planning using artificial potential field for waypoint tracking with collision avoidance,” in *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*, pp. 1–7, IEEE, 2020.

[325] J. Bao, X. Yao, H. Tang, and A. Song, “Outdoor navigation of a mobile robot by following gps waypoints and local pedestrian lane,” in *2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER)*, pp. 198–203, IEEE, 2018.

[326] J. Stanczak, D. Kozioł, I. Z. Kovács, J. Wigard, M. Wimmer, and R. Amorim, “Enhanced unmanned aerial vehicle communication support in lte-advanced,” in *2018 IEEE Conference on Standards for Communications and Networking (CSCN)*, pp. 1–6, IEEE, 2018.

[327] S. M. Hussain, K. M. Yusof, R. Asuncion, S. A. Hussain, and A. Ahmad, “An integrated approach of 4g lte and dsrc (ieee 802.11 p) for internet of vehicles (iov) by using a novel cluster-based efficient radio interface selection algorithm to improve vehicular network (vn) performance,” *Sustainable Advanced Computing*, pp. 569–583, 2022.

[328] R. Miyake, J. Kudo, E. Ishimura, H. Itoh, T. Yuzui, M. Shiokari, S. Kawashima, K. Hirata, Y. Niki, M. Kobayashi, *et al.*, “Application of dynamic-task-based hazard identification method to remote operation of experimental ship shinpo,” in *Journal of Physics: Conference Series*, vol. 2311, p. 012013, IOP Publishing, 2022.

[329] P. Purucker, J. Schmid, A. Höß, and B. W. Schuller, “System requirements specification for unmanned aerial vehicle (uav) to server communication,” in *2021 International Conference on Unmanned Aircraft Systems (ICUAS)*, pp. 1499–1508, IEEE, 2021.

[330] M. Storbacka, “Development of autonomous navigation systems for maritime applications,” 2021.

[331] M. Zhang, Z. Fan, R. Shibasaki, and X. Song, “Domain adversarial graph convolutional network based on rssi and crowdsensing for indoor localization,” *arXiv preprint arXiv:2204.05184*, 2022.

[332] K. Naheem, A. Elsharkawy, and M. S. Kim, “Tracking feasibility of uwb positioning system for lighter-than-air indoor robot navigation,” in *2021 21st International Conference on Control, Automation and Systems (ICCAS)*, pp. 2109–2111, IEEE, 2021.

[333] K. Mendes, “Research project 2: Drone-supported ai-based generation of 3d maps of indoor radio environments,” *arXiv preprint arXiv:2109.06923*, 2021.

[334] Y. Khassanov, M. Nurpeiissov, A. Sarkytbayev, A. Kuzdeuov, and H. A. Varol, “Finer-level sequential wifi-based indoor localization,” in *2021 IEEE/SICE International Symposium on System Integration (SII)*, pp. 163–169, IEEE, 2021.

[335] S. S. Dhanjal, M. Ghaffari, and R. M. Eustice, “Deeplocnet: Deep observation classification and ranging bias regression for radio positioning systems,” in *2019 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pp. 3802–3809, IEEE, 2019.

[336] Z. Ma, B. Wu, and S. Poslad, “A wifi rssi ranking fingerprint positioning system and its application to indoor activities of daily living recognition,” *International Journal of Distributed Sensor Networks*, vol. 15, no. 4, p. 1550147719837916, 2019.

[337] X. Zhao, X. Liao, Z. Wang, G. Wu, M. Barth, K. Han, and P. Tiwari, “Co-simulation platform for modeling and evaluating connected and automated vehicles and human behavior in mixed traffic,” *SAE Int. J. of CAV*, vol. 5, no. 4, 2022.

[338] L. Naik, S. Blumenthal, N. Huebel, H. Bruyninckx, and E. Prassler, “Semantic mapping extension for openstreetmap applied to indoor robot navigation,” in *2019 International Conference on Robotics and Automation (ICRA)*, pp. 3839–3845, IEEE, 2019.

[339] K. Weerakoon, A. J. Sathyamoorthy, U. Patel, and D. Manocha, “Terp: Reliable planning in uneven outdoor environments using deep reinforcement learning,” in *2022 International Conference on Robotics and Automation (ICRA)*, pp. 9447–9453, IEEE, 2022.

[340] S. Benders, “Reconfigurable path planning for fixed-wing unmanned aircraft using free-space roadmaps,” in *2018 International Conference on Unmanned Aircraft Systems (ICUAS)*, pp. 891–898, 2018.

[341] M. Kayton and W. R. Fried, *Avionics navigation systems*. John Wiley & Sons, 1997.

[342] K. Virrantaus, J. Markkula, A. Garmash, V. Terziyan, J. Veijalainen, A. Katanosov, and H. Tirri, “Developing gis-supported location-based services,” in *Proceedings of the Second International Conference on Web Information Systems Engineering*, vol. 2, pp. 66–75 vol.2, 2001.

[343] J. L. Crassidis and F. L. Markley, “New algorithm for attitude determination using global positioning system signals,” *Journal of Guidance, Control, and Dynamics*, vol. 20, no. 5, pp. 891–896, 1997.

[344] B. Wang, L. Miao, S. Wang, and J. Shen, “A constrained lambda method for gps attitude determination,” *GPS solutions*, vol. 13, no. 2, pp. 97–107, 2009.

[345] X. Liu, T. Ballal, H. Chen, and T. Y. Al-Naffouri, “Constrained wrapped least squares: A tool for high-accuracy gnss attitude determination,” *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–15, 2022.

[346] Y. Gan, L. Sui, G. Xiao, Q. Zhang, and L. Wang, “Real-time gnss attitude determination by a direct approach with efficiency and robustness,” *Measurement Science and Technology*, vol. 32, no. 11, p. 115904, 2021.

[347] L. He, W. Ma, P. Guo, and T. Sheng, “Developments of attitude determination and control system of microsats: A survey,” *Proceedings of the Institution of Mechanical Engineers, Part I: Journal of Systems and Control Engineering*, vol. 235, no. 10, pp. 1733–1750, 2021.

[348] I. Y. Bar-Itzhack, P. Y. Montgomery, and J. C. Garrick, “Algorithms for attitude determination using the global positioning system,” *Journal of guidance, control, and dynamics*, vol. 21, no. 6, pp. 846–852, 1998.

[349] J. R. Wertz, *Spacecraft attitude determination and control*, vol. 73. Springer Science & Business Media, 2012.

[350] F. L. Markley and J. L. Crassidis, *Fundamentals of spacecraft attitude determination and control*, vol. 1286. Springer, 2014.

[351] D. Gebre-Egziabher, R. Hayward, and J. Powell, “Design of multi-sensor attitude determination systems,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 40, no. 2, pp. 627–649, 2004.

[352] G. Lu, *Development of a GPS multi-antenna system for attitude determination.* University of Calgary Calgary, Canada, 1995.

[353] J. Murrell, “Precision attitude determination for multimission spacecraft,” in *Guidance and Control Conference*, p. 1248, 1978.

[354] R. Zhu, D. Sun, Z. Zhou, and D. Wang, “A linear fusion algorithm for attitude determination using low cost mems-based sensors,” *Measurement*, vol. 40, no. 3, pp. 322–328, 2007.

[355] J. Zhang, W. Meng, Q. Liu, H. Jiang, Y. Feng, and G. Wang, “Efficient vehicles path planning algorithm based on taxi gps big data,” *Optik*, vol. 127, no. 5, pp. 2579–2585, 2016.

[356] M. Maaref and Z. M. Kassas, “Optimal gps integrity-constrained path planning for ground vehicles,” in *2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, pp. 655–660, 2020.

[357] H. Lee, J. Seo, and Z. M. Kassas, “Integrity-based path planning strategy for urban autonomous vehicular navigation using gps and cellular signals,” in *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, pp. 2347–2357, 2020.

[358] G. S. Akhshirsh, N. K. Al-Salihi, and O. H. Hamid, “A cost-effective gps-aided autonomous guided vehicle for global path planning,” *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 2, pp. 650–657, 2021.

[359] P. Corcoran, “Topological path planning in gps trajectory data,” *Sensors*, vol. 16, no. 12, p. 2203, 2016.

[360] J. Wang, Y. Xiao, T. Li, and C. P. Chen, “Impacts of gps spoofing on path planning of unmanned surface ships,” *Electronics*, vol. 11, no. 5, p. 801, 2022.

[361] A. Al Arabi, H. Ul Sakib, P. Sarkar, T. P. Proma, J. Anowar, and M. A. Amin, “Autonomous rover navigation using gps based path planning,” in *2017 Asia Modelling Symposium (AMS)*, pp. 89–94, 2017.

[362] S. A. Korkmaz and M. Poyraz, “Path planning for rescue vehicles via segmented satellite disaster images and gps road map,” in *2016 9th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, pp. 145–150, 2016.

[363] C.-H. Chung, K.-C. Wang, K.-T. Liu, Y.-T. Wu, C.-C. Lin, and C.-Y. Chang, “Path planning algorithm for robotic lawnmower using rtk-gps localization,” in *2020 International Symposium on Community-centric Systems (CcS)*, pp. 1–4, 2020.

[364] Y. Li, T. Ma, P. Chen, Y. Jiang, R. Wang, and Q. Zhang, “Autonomous underwater vehicle optimal path planning method for seabed terrain matching navigation,” *Ocean Engineering*, vol. 133, pp. 107–115, 2017.

[365] Y. T. Tan, R. Gao, and M. Chitre, “Cooperative path planning for range-only localization using a single moving beacon,” *IEEE Journal of Oceanic Engineering*, vol. 39, no. 2, pp. 371–385, 2014.

[366] M. Imamura, R. Tomitaka, Y. Miyazaki, K. Kobayashi, and K. Watanabe, “Outdoor waypoint navigation for an intelligent wheelchair using differential gps and ins,” in *SICE 2004 Annual Conference*, vol. 3, pp. 2193–2196 vol. 3, 2004.

[367] A. M. Lekkas, “Guidance and path-planning systems for autonomous vehicles,” 2014.

[368] C. D. Crane III, A. L. Rankin, D. G. Armstrong II, J. S. Wit, and D. K. Novick, “An evaluation of ins and gps for autonomous navigation,” in *Intelligent Autonomous Vehicles 1995*, pp. 193–198, Elsevier, 1995.

[369] J. Golenbiewski and G. Tewolde, “Wi-fi based indoor positioning and navigation system (ips/ins),” in *2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, pp. 1–7, 2020.

[370] S. S. Ragothaman, *Path planning for autonomous ground vehicles using GNSS and cellular LTE signal reliability maps and GIS 3-D maps*. University of California, Riverside, 2018.

[371] S. Ragothaman, M. Maaref, and Z. M. Kassas, “Autonomous ground vehicle path planning in urban environments using gnss and cellular signals reliability maps: Simulation and experimental results,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 57, no. 4, pp. 2575–2586, 2021.

[372] X. Liu, T. Xi, E. Ngai, and W. Wang, “Path planning for aerial sensor networks with connectivity constraints,” in *2017 IEEE International Conference on Communications (ICC)*, pp. 1–6, 2017.

[373] S. Ragothaman, M. Maaref, and Z. M. Kassas, “Autonomous ground vehicle path planning in urban environments using gnss and cellular signals reliability maps: Models and algorithms,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 57, no. 3, pp. 1562–1580, 2021.

[374] R. Liu, D. Kwak, S. Devarakonda, K. Bekris, and L. Iftode, “Investigating remote driving over the lte network,” in *Proceedings of the 9th international conference on automotive user interfaces and interactive vehicular applications*, pp. 264–269, 2017.

[375] U. Challita, W. Saad, and C. Bettstetter, “Deep reinforcement learning for interference-aware path planning of cellular-connected uavs,” in *2018 IEEE International Conference on Communications (ICC)*, pp. 1–7, 2018.

[376] S. De Bast, E. Vinogradov, and S. Pollin, “Cellular coverage-aware path planning for uavs,” in *2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 1–5, 2019.

[377] F. Mezghani and N. Mitton, “Open problem: Energy-and time-efficient dynamic drone path planning for post-disaster network servicing,” in *ODS 2018-International Conference on Optimization and Decision Science*, 2018.

[378] S. Zhang and R. Zhang, “Radio map-based 3d path planning for cellular-connected uav,” *IEEE Transactions on Wireless Communications*, vol. 20, no. 3, pp. 1975–1989, 2021.

[379] Y. Shin and E. Kim, “Pf-dop hybrid path planning for safe and efficient navigation of unmanned vehicle systems,” in *Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018)*, pp. 2501–2517, 2018.

[380] H. Binol, E. Bulut, K. Akkaya, and I. Guvenc, “Time optimal multi-uav path planning for gathering its data from roadside units,” in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, pp. 1–5, 2018.

[381] A. M. de Souza, R. S. Yokoyama, G. Maia, A. Loureiro, and L. Villas, “Real-time path planning to prevent traffic jam through an intelligent transportation system,” in *2016 IEEE Symposium on Computers and Communication (ISCC)*, pp. 726–731, 2016.

[382] L. Shi, S. Xu, H. Liu, and Z. Zhan, “Qos-aware uav coverage path planning in 5g mmwave network,” *Computer Networks*, vol. 175, p. 107207, 2020.

[383] C. Almeida, T. Franco, H. Ferreira, A. Martins, R. Santos, J. M. Almeida, J. Carvalho, and E. Silva, “Radar based collision detection developments on usv roaz ii,” in *Oceans 2009-Europe*, pp. 1–6, Ieee, 2009.

[384] P. Biswas, M. Chakraborty, R. Bera, and S. Shome, “Ensuring reliability in vehicular collision avoidance using joint rfid and radar-based vehicle detection,” *Trends in Wireless Communication and Information Security*, pp. 99–105, 2021.

[385] A. Lazarowska, “Review of collision avoidance and path planning methods for ships utilizing radar remote sensing,” *Remote Sensing*, vol. 13, no. 16, p. 3265, 2021.

[386] R. Sivakumar and H. Mangalam, “Radar based vehicle collision avoidance system used in four wheeler automobile segments,” *International Journal of Scientific & Engineering Research*, vol. 5, no. 1, pp. 763–770, 2014.

[387] A.-P. Wang, J.-C. Chen, and P.-L. Hsu, “Intelligent can-based automotive collision avoidance warning system,” in *IEEE International Conference on Networking, Sensing and Control, 2004*, vol. 1, pp. 146–151, IEEE, 2004.

[388] R. Y. Gazit, *Aircraft surveillance and collision avoidance using GPS*. Stanford University, 1996.

[389] R. Toledo-Moreo and M. A. Zamora-Izquierdo, “Collision avoidance support in roads with lateral and longitudinal maneuver prediction by fusing gps/imu and digital maps,” *Transportation Research part C: emerging technologies*, vol. 18, no. 4, pp. 611–625, 2010.

[390] A. Nieto and K. Dagdelen, “Development and testing of a vehicle collision avoidance system based on gps and wireless networks for open-pit mines,” *Application of Computers and Operations Research in the Minerals Industries*, 2003.

[391] M.-P. Rudel and J. Baldwin, “Gps relative accuracy for collision avoidance,” in *Proceedings of the 1997 National Technical Meeting of The Institute of Navigation*, pp. 971–977, 1997.

[392] C.-P. Young, B.-R. Chang, H.-F. Tsai, R.-Y. Fang, J. Lin Jr, *et al.*, “Vehicle collision avoidance system using embedded hybrid intelligent prediction based on vision/gps sensing,” *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 12A, pp. 4453–4468, 2009.

[393] Y. Sato, Y. Shimonaka, T. Maruoka, T. Wada, and H. Okada, “Vehicular collision avoidance support system v2 (vcassv2) by gps+ins hybrid vehicular positioning method,” in *2007 Australasian Telecommunication Networks and Applications Conference*, pp. 29–34, 2007.

[394] K. Kose, C. Yang, Y. Ishioka, Y. Kato, A. Nagasawa, and K. Hara, “A collision avoidance expert system for integrated navigation system and its brush-up,” *Journal of the Society of Naval architects of Japan*, vol. 1995, no. 177, pp. 399–407, 1995.

[395] H. Elsayed, B. A. Abdullah, and G. Aly, “Fuzzy logic based collision avoidance system for autonomous navigation vehicle,” in *2018 13th International Conference on Computer Engineering and Systems (ICCES)*, pp. 469–474, 2018.

[396] J. Igual, M. Catalan, M. Catalan-Cid, F. Vázquez-Gallego, J. Fernández, R. Muñoz, R. Sedar, R. Casellas, R. Vilalta, A. Calveras, J. Paradells, M. Lefebvre, F. Gardes, J.-M. Odinot, F. Moscatelli, G. Landi, S. K. Datta, J. Härri, R. Silva, and X. Vilajosana, “Demonstration and evaluation of precise positioning for connected and automated mobility services,” in *2022 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, pp. 267–272, 2022.

[397] N. Alam, A. T. Balaie, and A. G. Dempster, “Dynamic path loss exponent and distance estimation in a vehicular network using doppler effect and received signal strength,” in *2010 IEEE 72nd Vehicular Technology Conference - Fall*, pp. 1–5, 2010.

[398] A. Paier, L. Bernadó, J. Karedal, O. Klemp, and A. Kwoczek, “Overview of vehicle-to-vehicle radio channel measurements for collision avoidance applications,” in *2010 IEEE 71st Vehicular Technology Conference*, pp. 1–5, 2010.

[399] A. Viquerat, L. Blackhall, A. Reid, S. Sukkarieh, and G. Brooker, “Reactive collision avoidance for unmanned aerial vehicles using doppler radar,” in *Field and Service Robotics*, pp. 245–254, Springer, 2008.

[400] J. Huang, Y.-H. Lee, T.-W. Lin, Y.-L. Chen, Y.-D. Liao, H.-W. Tseng, and Y.-S. Ho, “The use of doppler effect in early warning system for vehicle collision at crossroad,” *Microsystem Technologies*, vol. 27, no. 4, pp. 1711–1720, 2021.

[401] B. Kihei, J. A. Copeland, and Y. Chang, “Automotive doppler sensing: The doppler profile with machine learning in vehicle-to-vehicle networks for road safety,” in *2017 IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 1–5, 2017.

[402] J. He, Z. Tang, Z. Fan, and J. Zhang, “Enhanced collision avoidance for distributed lte vehicle to vehicle broadcast communications,” *IEEE Communications Letters*, vol. 22, no. 3, pp. 630–633, 2018.

[403] J. Li, Y. Zhang, M. Shi, Q. Liu, and Y. Chen, “Collision avoidance strategy supported by lte-v-based vehicle automation and communication systems for car following,” *Tsinghua Science and Technology*, vol. 25, no. 1, pp. 127–139, 2019.

[404] N. Mouawad, V. Mannoni, B. Denis, and A. P. da Silva, “Impact of lte-v2x connectivity on global occupancy maps in a cooperative collision avoidance (coca) system,” in *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, pp. 1–5, IEEE, 2021.

[405] H. A. Halim, A. R. M. Shariff, S. I. Fadilah, and F. Karim, “Performance evaluation of safe avoidance time and safety message dissemination for vehicle to vehicle (v2v) communication in lte c-v2x,” *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 3, 2022.

[406] R.-A. Rill and K. B. Faragó, “Collision avoidance using deep learning-based monocular vision,” *SN Computer Science*, vol. 2, no. 5, pp. 1–10, 2021.

[407] K. Hatch, J. M. Mern, and M. J. Kochenderfer, “Obstacle avoidance using a monocular camera,” in *AIAA Scitech 2021 Forum*, p. 0269, 2021.

[408] M. Mahmeen, R. D. D. Sanchez, M. Friebe, M. Pech, and S. Haider, “Collision avoidance route planning for autonomous medical devices using multiple depth cameras,” *IEEE Access*, vol. 10, pp. 29903–29915, 2022.

[409] A. H. Sawalmeh and N. S. Othman, “An overview of collision avoidance approaches and network architecture of unmanned aerial vehicles (uavs),” *arXiv preprint arXiv:2103.14497*, 2021.

[410] S. S. Tikar and R. A. Patil, “A novel fast responding driver assistance technique with efficient lane detection and collision avoidance using dynamic feature extraction in any environment.,” *Traitement du Signal*, vol. 39, no. 2, 2022.

[411] W. Jansen, D. Laurijssen, and J. Steckel, “Real-time sonar fusion for layered navigation controller,” *Sensors*, vol. 22, no. 9, p. 3109, 2022.

[412] J. Wouter, L. Dennis, and S. Jan, “Adaptive acoustic flow-based navigation with 3d sonar sensor fusion,” in *2021 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, pp. 1–8, IEEE, 2021.

[413] R. Kot, “Review of collision avoidance and path planning algorithms used in autonomous underwater vehicles,” *Electronics*, vol. 11, no. 15, p. 2301, 2022.

[414] X. Cao, L. Ren, and C. Sun, “Research on obstacle detection and avoidance of autonomous underwater vehicle based on forward-looking sonar,” *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1–11, 2022.

[415] J. Fang, X. Zuo, D. Zhou, S. Jin, S. Wang, and L. Zhang, “Lidar-aug: A general rendering-based augmentation framework for 3d object detection,” in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 4710–4720, 2021.

[416] J.-S. Kim, D.-H. Lee, D.-W. Kim, H. Park, K.-J. Paik, and S. Kim, “A numerical and experimental study on the obstacle collision avoidance system using a 2d lidar sensor for an autonomous surface vehicle,” *Ocean Engineering*, vol. 257, p. 111508, 2022.

[417] M. Beul and S. Behnke, “Trajectory generation with fast lidar-based 3d collision avoidance for agile mavs,” in *2020 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR)*, pp. 42–48, IEEE, 2020.

[418] J. Enayati, P. Asef, and Y. Jonnalagadda, “A novel triple radar arrangement for level 2 adas detection system in autonomous vehicles,” 2022.

[419] N. Horri, O. Haas, S. Wang, M. Foo, and M. S. Fernandez, “Mode switching control using lane keeping assist and waypoints tracking for autonomous driving in a city environment,” *Transportation research record*, vol. 2676, no. 3, pp. 712–727, 2022.

[420] J. H. Yang, W. Y. Choi, and C. C. Chung, “Driving environment assessment and decision making for cooperative lane change system of autonomous vehicles,” *Asian Journal of Control*, vol. 23, no. 3, pp. 1135–1145, 2021.

[421] Z. F. Magosi, H. Li, P. Rosenberger, L. Wan, and A. Eichberger, “A survey on modelling of automotive radar sensors for virtual test and validation of automated driving,” *Sensors*, vol. 22, no. 15, p. 5693, 2022.

[422] D. J. Kim, J. S. Kim, J. H. Yang, S. C. Kee, and C. C. Chung, “Lane change intention classification of surrounding vehicles utilizing open set recognition,” *IEEE Access*, vol. 9, pp. 57589–57602, 2021.

[423] Z. Feng, M. Stolz, M. Li, M. Kunert, and W. Wiesbeck, “Verification of a lane detection method with automotive radar based on a new type of road marking,” in *2018 IEEE MTT-S International Conference on Microwaves for Intelligent Mobility (ICMIM)*, pp. 1–4, IEEE, 2018.

[424] N. B. Chetan, J. Gong, H. Zhou, D. Bi, J. Lan, and L. Qie, “An overview of recent progress of lane detection for autonomous driving,” in *2019 6th International conference on dependable systems and their applications (DSA)*, pp. 341–346, IEEE, 2020.

[425] R. Philipp, F. Schuldt, and F. Howar, “Functional decomposition of automated driving systems for the classification and evaluation of perceptual threats,” in *13. Uni-DAS eV Workshop Fahrerassistenz und automatisiertes Fahren 2020*, Walting, 2020.

[426] T. K. Nagy and E. Costa, “Development of a lane keeping steering control by using camera vanishing point strategy,” *Multidimensional Systems and Signal Processing*, vol. 32, no. 2, pp. 845–861, 2021.

[427] R. Romano, D. Maggi, T. Hirose, Z. Broadhead, and O. Carsten, “Impact of lane keeping assist system camera misalignment on driver behavior,” *Journal of Intelligent Transportation Systems*, vol. 25, no. 2, pp. 157–169, 2020.

[428] M. R. Cantas and L. Guvenc, “Camera based automated lane keeping application complemented by gps localization based path following,” *SAE Technical Paper Series*, vol. 1, 2018.

[429] N. C. Basjaruddin, E. Rakhman, and F. Adinugraha, “Hardware simulation of lane keeping assist based on sensor fusion,” *International Journal of Intelligent Unmanned Systems*, 2020.

[430] C. Lin, Y. Guo, W. Li, H. Liu, and D. Wu, “An automatic lane marking detection method with low-density roadside lidar data,” *IEEE Sensors Journal*, vol. 21, no. 8, pp. 10029–10038, 2021.

[431] V. Pagire and S. Mate, “Autonomous vehicle using computer vision and lidar,” *i-Manager’s Journal on Embedded Systems*, vol. 9, no. 2, p. 7, 2021.

[432] K. Li, X. Yang, Y. Luo, and H. Li, “Road geometry perception without accurate positioning and lane information,” *IET Intelligent Transport Systems*, 2022.

[433] F. H. Shadeed and S. J. Wallaschek, “Concept of an intelligent adaptive vehicle front-lighting assistance system,” in *2007 IEEE Intelligent Vehicles Symposium*, pp. 1118–1121, IEEE, 2007.

[434] O. U. KURTULUŞ, “The exterior lighting systems for automated vehicle’s communication with pedestrian and vehicle to vehicle,” *www. imstec. org*, p. 12.

[435] A. Radoš, Z. Krpić, V. Marinković, and N. Lukić, “Modeling and implementation of an adaptive vehicle light management system,” in *2021 Zooming Innovation in Consumer Technologies Conference (ZINC)*, pp. 75–80, IEEE, 2021.

[436] P. Dubal and J. Nanaware, “Design of adaptive headlights for automobiles,” *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 3, no. 3, pp. 1599–1603, 2015.

[437] S. G. Magar, “Adaptive front light systems of vehicle for road safety,” in *2015 International Conference on Computing Communication Control and Automation*, pp. 551–554, IEEE, 2015.

[438] S. Li and L. Zhao, “A low-cost and fast vehicle detection algorithm with a monocular camera for adaptive driving beam systems,” *IEEE Access*, vol. 9, pp. 26147–26155, 2021.

[439] G. Toney *et al.*, “Design & implementation of smart headlamps, overtaking assistance for automobiles using matlab,” *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 10, pp. 286–293, 2021.

[440] C. Rongier, R. Gilblas, Y. Le Maoult, S. Belkessam, and F. Schmidt, “Infrared thermography applied to the validation of thermal simulation of high luminance led used in automotive front lighting,” *Infrared Physics & Technology*, vol. 120, p. 103980, 2022.

[441] J. Zhao, J. Fang, S. Wang, K. Wang, C. Liu, and T. Han, “Obstacle avoidance of multi-sensor intelligent robot based on road sign detection,” *Sensors*, vol. 21, no. 20, p. 6777, 2021.

[442] R. Yazdan and M. Varshosaz, “Improving traffic sign recognition results in urban areas by overcoming the impact of scale and rotation,” *ISPRS Journal of Photogrammetry and Remote Sensing*, vol. 171, pp. 18–35, 2021.

[443] H. Le, M. Nguyen, W. Q. Yan, and S. Lo, “Training a convolutional neural network for transportation sign detection using synthetic dataset,” in *2021 36th International Conference on Image and Vision Computing New Zealand (IVCNZ)*, pp. 1–6, IEEE, 2021.

[444] N. Hasan, T. Anzum, and N. Jahan, “Traffic sign recognition system (tsrs): Svm and convolutional neural network,” in *Inventive communication and computational technologies*, pp. 69–79, Springer, 2021.

[445] M. Dhelia, S. Chaughule, A. Choraria, A. Hariharan, and M. M. Pai, “Protall (an intelligent, multi-sensor, comprehensive obstacle avoidance system for automobiles and uavs),” in *Journal of Physics: Conference Series*, vol. 2161, p. 012056, IOP Publishing, 2022.

[446] R. V. KAMBLE and S. PATIL, “Intelligent night vision system for automobile based on computer vision,” *JournalNX*, vol. 2, no. 10, pp. 23–27.

[447] K. Priyadharshini, D. Aswanthi, X. Sheela, K. Subhanu, *et al.*, “Surveillance based spotting and categorization of automobiles,” in *2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)*, pp. 37–42, IEEE, 2022.

[448] M. Wang, X. Chen, B. Jin, P. Lv, W. Wang, and Y. Shen, “A novel v2v cooperative collision warning system using uwb/dr for intelligent vehicles,” *Sensors*, vol. 21, no. 10, p. 3485, 2021.

[449] A. Ahamed, N. Islam, M. A. S. Soikot, M. S. Hossen, R. Ahmed, and M. A. Hasan, “Train collision avoidance using gps and gsm module,” in *2019 International Conference on Power Electronics, Control and Automation (ICPECA)*, pp. 1–4, IEEE, 2019.

[450] A. Guizar, V. Mannoni, F. Poli, B. Denis, and V. Berg, “Lte-v2x performance evaluation for cooperative collision avoidance (coca) systems,” in *2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*, pp. 1–5, IEEE, 2020.

[451] J. Kim, “Reactive control for collision evasion with extended obstacles,” *Sensors*, vol. 22, no. 15, p. 5478, 2022.

[452] A. Shalumov, R. Halaly, and E. E. Tsur, “Lidar-driven spiking neural network for collision avoidance in autonomous driving,” *Bioinspiration & Biomimetics*, vol. 16, no. 6, p. 066016, 2021.

[453] C. Lin, Y. Guo, W. Li, H. Liu, and D. Wu, “An automatic lane marking detection method with low-density roadside lidar data,” *IEEE Sensors Journal*, vol. 21, no. 8, pp. 10029–10038, 2021.

[454] T. Alsuwian, R. B. Saeed, and A. A. Amin, “Autonomous vehicle with emergency braking algorithm based on multi-sensor fusion and super twisting speed controller,” *Applied Sciences*, vol. 12, no. 17, p. 8458, 2022.

[455] D. Tagliaferri, M. Rizzi, S. Tebaldini, M. Nicoli, I. Russo, C. Mazzucco, A. V. Monti-Guarnieri, C. M. Prati, and U. Spagnolini, “Cooperative synthetic aperture radar in an urban connected car scenario,” in *2021 1st IEEE International Online Symposium on Joint Communications & Sensing (JC&S)*, pp. 1–4, IEEE, 2021.

[456] S. Rajendar and V. K. Kaliappan, “Recent advancements in autonomous emergency braking: A survey,” in *2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, pp. 1027–1032, IEEE, 2021.

[457] Y. Choi, S. Baek, C. Kim, J. Yoon, and S. M. Lee, “Simulation of aebs applicability by changing radar detection angle,” *Applied Sciences*, vol. 11, no. 5, p. 2305, 2021.

[458] L. Carabulea, C. Pozna, C. Antonya, C. Husar, and A. Băicoianu, “The influence of the advanced emergency braking system in critical scenarios for autonomous vehicles,” in *IOP Conference Series: Materials Science and Engineering*, vol. 1220, p. 012045, IOP Publishing, 2022.

[459] M. Gawande, P. Rajalakshmi, *et al.*, “Autonomous emergency breaking (aeb) evaluation for indian traffic scenarios using gps and lidar data,” in *2022 IEEE IAS Global Conference on Emerging Technologies (GlobConET)*, pp. 655–660, IEEE, 2022.

[460] T. Li, Z. Yao, Z. Ji, and H. Ji, "Analysis of braking effect of advanced driver assistance system in the scenario of cut-in," in *International Conference on Smart Transportation and City Engineering 2021*, vol. 12050, pp. 1411–1419, SPIE, 2021.

[461] R. Kapse and S. Adarsh, "Implementing an autonomous emergency braking with simulink using two radar sensors," *arXiv preprint arXiv:1902.11210*, 2019.

[462] S. Rajendar, D. Rathinasamy, R. Pavithra, V. K. Kaliappan, and S. Gnanamurthy, "Prediction of stopping distance for autonomous emergency braking using stereo camera pedestrian detection," *Materials Today: Proceedings*, vol. 51, pp. 1224–1228, 2022.

[463] M. Ariyanto, G. D. Haryadi, M. Munadi, R. Ismail, and Z. Hendra, "Development of low-cost autonomous emergency braking system (aebs) for an electric car," in *2018 5th International Conference on Electric Vehicular Technology (ICEVT)*, pp. 167–171, IEEE, 2018.

[464] E. Priyanka, S. Thangavel, S. Tharun, S. N. Saravanan, S. R. Sankar, B. B. Kumar, and C. Pugazhenthi, "Iot based rash braking data analysis and plotting in google maps using raspberry pi," in *2021 International Conference on Data Analytics for Business and Industry (ICDABI)*, pp. 320–325, IEEE, 2021.

[465] G. Mehta, Y. Mishra, U. Ashraf, S. Dubey, M. Singh, and R. Khanam, "Accident prevention using an auto braking system and accident detection using internet of things," in *Smart Computing*, pp. 142–148, CRC Press, 2021.

[466] Z. Song, L. Cao, and C. C. Chou, "Development of test equipment for pedestrian-automatic emergency braking based on c-ncap (2018)," *Sensors*, vol. 20, no. 21, p. 6206, 2020.

[467] J. Ciberlin, R. Grbic, N. Teslić, and M. Pilipović, "Object detection and object tracking in front of the vehicle using front view camera," in *2019 Zooming Innovation in Consumer Technologies Conference (ZINC)*, pp. 27–32, IEEE, 2019.

[468] R. Chowdhury, Z. Islam, S. D. Rozario, Z. Mohammad, and M. I. Ema, "Automated self driving car following lane with emergency braking system," in *Proceedings of the International Conference on Computing Advancements*, pp. 1–4, 2020.

[469] J. J. Chico, M. A. Doron, A. R. Infante, G. N. Verdey, R. D. Umali, M. C. E. Manuel, R. S. Pangantihon, and J. F. Villaverde, "Design, fabrication, and testing of an automated pneumatic braking program with the use of ultrasonic sensor," in *2021 IEEE 13th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM)*, pp. 1–6, IEEE, 2021.

[470] J. Zhao, Y. Li, B. Zhu, W. Deng, and B. Sun, "Method and applications of lidar modeling for virtual testing of intelligent vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 5, pp. 2990–3000, 2020.

[471] T. S. Combs, L. S. Sandt, M. P. Clamann, and N. C. McDonald, "Automated vehicles and pedestrian safety: exploring the promise and limits of pedestrian detection," *American journal of preventive medicine*, vol. 56, no. 1, pp. 1–7, 2019.

[472] Z. Zhang, X. Wang, D. Huang, X. Fang, M. Zhou, and Y. Zhang, "Mrpt: Millimeter-wave radar-based pedestrian trajectory tracking for autonomous urban driving," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–17, 2021.

[473] T. Kawanishi, S. Masuda, K. Jitsuno, K. Inagaki, and A. Kanno, "Secondary radar using frequency doubling for non-line-of-sight pedestrian detection," in *2021 IEEE Conference on Antenna Measurements & Applications (CAMA)*, pp. 466–467, IEEE, 2021.

[474] P. Held, D. Steinhauser, A. Koch, T. Brandmeier, and U. T. Schwarz, "A novel approach for model-based pedestrian tracking using automotive radar," *IEEE Transactions on Intelligent Transportation Systems*, 2021.

[475] J. P. Lima, R. Roberto, L. Figueiredo, F. Simoes, and V. Teichrieb, “Generalizable multi-camera 3d pedestrian detection,” in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pp. 1232–1240, 2021.

[476] F. Altay and S. Velipasalar, “The use of thermal cameras for pedestrian detection,” *IEEE Sensors Journal*, 2022.

[477] J. Wan, M. Xia, Z. Huang, L. Tian, X. Zheng, V. Chang, Y. Zhu, and H. Wang, “Event-based pedestrian detection using dynamic vision sensors,” *Electronics*, vol. 10, no. 8, p. 888, 2021.

[478] X. Dai, J. Hu, H. Zhang, A. Shitu, C. Luo, A. Osman, S. Sfarra, and Y. Duan, “Multi-task faster r-cnn for nighttime pedestrian detection and distance estimation,” *Infrared Physics & Technology*, vol. 115, p. 103694, 2021.

[479] C. V. Kieu, N. N. Pham, A. T. Le, A. S. Le, and X. N. Ho, “An overview of pedestrian detection based on lidar for advanced driving assistance system,” in *Regional Conference in Mechanical Manufacturing Engineering*, pp. 352–363, Springer, 2022.

[480] X. Peng and J. Shan, “Detection and tracking of pedestrians using doppler lidar,” *Remote Sensing*, vol. 13, no. 15, p. 2952, 2021.

[481] C. Xiang, L. Zhang, X. Xie, L. Zhao, X. Ke, Z. Niu, and F. Wang, “Multi-sensor fusion algorithm in cooperative vehicle-infrastructure system for blind spot warning,” *International Journal of Distributed Sensor Networks*, vol. 18, no. 5, p. 15501329221100412, 2022.

[482] S. Hayashi, K. Saho, D. Isobe, and M. Masugi, “Pedestrian detection in blind area and motion classification based on rush-out risk using micro-doppler radar,” *Sensors*, vol. 21, no. 10, p. 3388, 2021.

[483] H. M. Thakurdesai and J. V. Aghav, “Autonomous cars: technical challenges and a solution to blind spot,” in *Advances in Computational Intelligence and Communication Technology*, pp. 533–547, Springer, 2021.

[484] R. J. Jansen and S. F. Varotto, “Caught in the blind spot of a truck: A choice model on driver glance behavior towards cyclists at intersections,” *Accident Analysis & Prevention*, vol. 174, p. 106759, 2022.

[485] M. Kobayashi and N. Motoi, “Path planning method considering blind spots based on ros navigation stack and dynamic window approach for wheeled mobile robot,” in *2022 International Power Electronics Conference (IPEC-Himeji 2022-ECCE Asia)*, pp. 274–279, IEEE, 2022.

[486] K. S. Pawar, S. N. Teli, P. Shetye, S. Shetty, V. Satam, and A. Sahani, “Blind-spot monitoring system using lidar,” *Journal of The Institution of Engineers (India): Series C*, pp. 1–12, 2022.

[487] G. Popa, M.-A. Ghe□i, E. Tudor, I. Vasile, and I.-C. Sburlan, “Experimental study regarding long range lidar capabilities in sensing safety distance for vehicle application,” *Sensors*, vol. 22, no. 15, p. 5731, 2022.

[488] X. Kuang, Y. Zhang, and X. Wang, “System design of automatic parking assist based on iso26262,” in *Journal of Physics: Conference Series*, vol. 2195, p. 012032, IOP Publishing, 2022.

[489] B. Lei, S. Zhang, R. Liang, and H. Geng, “Research on subjective evaluation method of intelligent parking assist system based on typical parking scenario,” in *E3S Web of Conferences*, vol. 268, p. 01038, EDP Sciences, 2021.

[490] A. J. James and K. Jayavel, “Automotive radar human classification algorithm through simulation analysis: Basics and practical challenges,” in *High Performance Computing and Networking*, pp. 575–590, Springer, 2022.

[491] Z. Benyahia, M. Hefnawi, M. Aboulfatah, E. Abdelmounim, and T. Gadi, “Squeezenet-based range, angle, and doppler estimation for automotive mimo radar systems,” in *2022 International Conference on Intelligent Systems and Computer Vision (ISCV)*, pp. 1–5, IEEE, 2022.

[492] N. Pandey and S. S. Ram, “Automated parking test using isar images from automotive radar,” in *2021 IEEE International Conference on Autonomous Systems (ICAS)*, pp. 1–5, IEEE, 2021.

[493] H. Iqbal, A. Löffler, M. N. Mejdoub, D. Zimmermann, and F. Gruson, “Imaging radar for automated driving functions,” *International Journal of Microwave and Wireless Technologies*, vol. 13, no. 7, pp. 682–690, 2021.

[494] L. Hu and Z. Liu, “Intelligent parking lot assistance system based on machine vision and a□ algorithm,” in *2021 3rd International Symposium on Smart and Healthy Cities (ISHC)*, pp. 28–35, IEEE, 2021.

[495] D. Nugraha, F. Ahmed, M. Abdullah, and M. Johar, “Survey of smart parking application deployment,” in *IOP Conference Series: Materials Science and Engineering*, vol. 1108, p. 012019, IOP Publishing, 2021.

[496] S. Vasantha and J. Kunuthuru, “Parking assistance system,” 2021.

[497] R. Easley and S. M. Rahman, “Developing safety metrics for automatic vehicle parking using machine learning,” in *2021 IEEE International Workshop on Metrology for Automotive (MetroAutomotive)*, pp. 19–24, IEEE, 2021.

[498] F. A. A. Aziz, S. Z. M. Muji, M. H. Abd Wahab, Z. Tukiran, C. Uttrapan, *et al.*, “Smart parking system mobile application using ultrasonic detector,” *International Journal of Integrated Engineering*, vol. 14, no. 3, pp. 70–79, 2022.

[499] M. Kuprešak, M. Vranješ, D. Vajak, and D. Živkov, “Solution for autonomous vehicle parking,” in *2021 International Symposium ELMAR*, pp. 65–70, IEEE, 2021.

[500] R. Roriz, J. Cabral, and T. Gomes, “Automotive lidar technology: A survey,” *IEEE Transactions on Intelligent Transportation Systems*, 2021.

[501] V. Kamalkumar, S. Sonali, V. Sindhuja, and A. Sriharish, “Lidar based self driving car,” in *Proceedings of the International Conference on Intelligent Technologies in Security and Privacy for Wireless Communication, ITSPWC 2022, 14-15 May 2022, Karur, Tamilnadu, India*, 2022.

[502] L. P. Peláez, M. E. V. Recalde, E. D. M. Muñóz, J. M. Larrauri, J. M. P. Rastelli, N. Druml, and B. Hillbrand, “Car parking assistance based on time-or-flight camera,” in *2019 IEEE Intelligent Vehicles Symposium (IV)*, pp. 1753–1759, IEEE, 2019.

[503] J. Martinez, D. Zoeke, and M. Vossiek, “Convolutional neural networks for parking space detection in downfire urban radar,” *International Journal of Microwave and Wireless Technologies*, vol. 10, no. 5-6, pp. 643–650, 2018.

[504] B.-X. Wu, J.-J. Lin, H.-K. Kuo, P.-Y. Chen, and J.-I. Guo, “Radar and camera fusion for vacant parking space detection,” in *2022 IEEE 4th International Conference on Artificial Intelligence Circuits and Systems (AICAS)*, pp. 242–245, IEEE, 2022.

[505] Y. Ma, Y. Liu, L. Zhang, Y. Cao, S. Guo, and H. Li, “Research review on parking space detection method,” *Symmetry*, vol. 13, no. 1, p. 128, 2021.

[506] Z. Cai, Y. Zhou, Y. Qi, W. Zhuang, and L. Deng, “A millimeter wave dual-lens antenna for iot-based smart parking radar system,” *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 418–427, 2020.

[507] R. Wang, J. Pei, Y. Zhang, M. Li, Y. Huang, and J. Wu, “An auxiliary parking method based on automotive millimeter wave sar,” in *IGARSS 2019-2019 IEEE International Geoscience and Remote Sensing Symposium*, pp. 2503–2506, IEEE, 2019.

[508] K. Yugesh and C.-S. Kang, “A connected car-based parking location service system,” in *2019 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*, pp. 167–171, IEEE, 2019.

[509] B. Shin, J. H. Lee, T. Lee, and C. Kee, “Lte signal based vehicle localization in indoor parking lot using mobile phone,” in *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, pp. 378–415, 2019.

[510] K. Yugesh and C. S. Kang, “A novel connected vehicle-based parking space guidance system,” □□□□□□□□□, vol. 45, no. 7, pp. 1277–1292, 2020.

[511] B. Shin, J. H. Lee, C. Yu, C. Kim, and T. Lee, “Underground parking lot navigation system using long-term evolution signal,” *Sensors*, vol. 21, no. 5, p. 1725, 2021.

[512] H. Bura, N. Lin, N. Kumar, S. Malekar, S. Nagaraj, and K. Liu, “An edge based smart parking solution using camera networks and deep learning,” in *2018 IEEE International Conference on Cognitive Computing (ICCC)*, pp. 17–24, IEEE, 2018.

[513] C.-F. Peng, J.-W. Hsieh, S.-W. Leu, and C.-H. Chuang, “Drone-based vacant parking space detection,” in *2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pp. 618–622, IEEE, 2018.

[514] K. Gkolias and E. I. Vlahogianni, “Convolutional neural networks for on-street parking space detection in urban networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 12, pp. 4318–4327, 2018.

[515] A. Farley, H. Ham, *et al.*, “Real time ip camera parking occupancy detection using deep learning,” *Procedia Computer Science*, vol. 179, pp. 606–614, 2021.

[516] C. Zhang and B. Du, “Image-based approach for parking-spot detection with occlusion handling,” *Journal of Transportation Engineering, Part A: Systems*, vol. 146, no. 9, p. 04020098, 2020.

[517] S. Gören, D. F. Óncevarlk, K. D. Yldz, and T. Z. Hakyemez, “On-street parking spot detection for smart cities,” in *2019 IEEE International Smart Cities Conference (ISC2)*, pp. 292–295, IEEE, 2019.

[518] Z. Gong, J. Li, Z. Luo, C. Wen, C. Wang, and J. Zelek, “Mapping and semantic modeling of underground parking lots using a backpack lidar system,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 2, pp. 734–746, 2019.

[519] K. Park, G. Im, M. Kim, and J. Park, “Parking space detection based on camera and lidar sensor fusion,” *The Journal of Korea Robotics Society*, vol. 14, no. 3, pp. 170–178, 2019.

[520] G. Im, M. Kim, and J. Park, “Parking line based slam approach using avm/lidar sensor fusion for rapid and accurate loop closing and parking space detection,” *Sensors*, vol. 19, no. 21, p. 4811, 2019.

[521] C. Yuan, L. Fei, C. Jianxin, and J. Wei, “A smart parking system using wifi and wireless sensor network,” in *2016 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*, pp. 1–2, 2016.

[522] C.-F. Yang, Y.-H. Ju, C.-Y. Hsieh, C.-Y. Lin, M.-H. Tsai, and H.-L. Chang, “iparking – a real-time parking space monitoring and guiding system,” *Vehicular Communications*, vol. 9, pp. 301–305, 2017.

[523] Y. Agarwal, P. Ratnani, U. Shah, and P. Jain, “Iot based smart parking system,” in *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, pp. 464–470, 2021.

[524] C. Diehl, A. Makarow, C. Rösmann, and T. Bertram, “Time-optimal nonlinear model predictive control for radar-based automated parking,” *IFAC-PapersOnLine*, vol. 55, no. 14, pp. 34–39, 2022. 11th IFAC Symposium on Intelligent Autonomous Vehicles IAV 2022.

[525] J. Zhang, M. Zhang, Z. Fang, Y. Wang, X. Zhao, and S. Pu, “Rvdet: Feature-level fusion of radar and camera for object detection,” in *2021 IEEE International Intelligent Transportation Systems Conference (ITSC)*, pp. 2822–2828, 2021.

[526] S. Solmaz, R. Muminovic, A. Civgin, and G. Stettinger, “Development, analysis, and real-life benchmarking of rrt-based path planning algorithms for automated valet parking,” in *2021 IEEE International Intelligent Transportation Systems Conference (ITSC)*, pp. 621–628, 2021.

[527] Y. Kang, Y. Song, W. Ge, and T. Ling, “Robust multi-camera slam with manhattan constraint toward automated valet parking,” in *2021 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pp. 7615–7622, 2021.

[528] M. Khalid, K. Wang, N. Aslam, Y. Cao, N. Ahmad, and M. K. Khan, “From smart parking towards autonomous valet parking: A survey, challenges and future works,” *Journal of Network and Computer Applications*, vol. 175, p. 102935, 2021.

[529] H. Ryu, B. Kim, H. Yoo, and J. Lee, “Fully automated valet parking system based on infrastructure sensing,” in *RiTA 2020* (E. Chew, A. P. P. Abdul Majeed, P. Liu, J. Platts, H. Myung, J. Kim, and J.-H. Kim, eds.), (Singapore), pp. 22–31, Springer Singapore, 2021.

[530] T. Tiong, I. Saad, K. T. K. Teo, and H. Bin Lago, “Autonomous valet parking with asynchronous advantage actor-critic proximal policy optimization,” in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0334–0340, 2022.

[531] J. Scholliers, P. Pyykönen, A. Virtanen, E. Aittoniemi, F. Malin, M. Federley, and S. Nikolaou, *Automated Valet Parking using IoT: Design, user experience and business opportunities*, p. 68. No. 7/2020 in Traficom Research Reports, Finland: Liikenne- ja viestintävirasto Traficom, April 2020. 8th Transport Research Arena, TRA 2020 - Conference cancelled, TRA 2020 ; Conference date: 27-04-2020 Through 30-04-2020.

[532] M. Sakr, A. Moussa, W. Abdelfatah, M. Elsheikh, A. Noureldin, and N. El-Sheimy, “Radar-based multi-floor localization for automated valet parking,” in *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, pp. 647–673, 2020.

[533] J. Yu and J. Su, “Visual place recognition via semantic and geometric descriptor for automated valet parking,” in *2021 IEEE International Conference on Robotics and Biomimetics (ROBIO)*, pp. 1142–1147, 2021.

[534] C. Zhang, H. Liu, Z. Xie, K. Yang, K. Guo, R. Cai, and Z. Li, “Avp-loc: Surround view localization and relocalization based on hd vector map for automated valet parking,” in *2021 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pp. 5552–5559, 2021.

[535] J. Liu and J. Liu, “Intelligent and connected vehicles: Current situation, future directions, and challenges,” *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 59–65, 2018.

[536] Z. El-Rewini, K. Sadatsharan, N. Sugunaraj, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, “Cybersecurity attacks in vehicular sensors,” *IEEE Sensors Journal*, vol. 20, no. 22, pp. 13752–13767, 2020.

[537] H. Vdovic, J. Babic, and V. Podobnik, “Automotive software in connected and autonomous electric vehicles: A review,” *IEEE Access*, vol. 7, pp. 166365–166379, 2019.

[538] S. Karthikeyan, S. R. Srinivasan, J. Syed Ali, and A. Veeraraghavan, “Smart summoning of ambulance during a vehicle accident,” in *2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT)*, pp. 418–423, 2018.

[539] W. L. Leong, N. Martinel, S. Huang, C. Micheloni, G. L. Foresti, and R. Teo, “Integrated perception and tactical behaviours in an auto-organizing aerial sensor network,” in *2020 International Conference on Unmanned Aircraft Systems (ICUAS)*, pp. 429–438, 2020.

[540] R. Donà, K. Mattas, Y. He, G. Albano, and B. Ciuffo, “Multianticipation for string stable adaptive cruise control and increased motorway capacity without vehicle-to-vehicle communication,” *Transportation Research Part C: Emerging Technologies*, vol. 140, p. 103687, 2022.

[541] P. K. Dyakov, A. N. Andreev, A. M. Ivanov, and A. I. Kalinin, “Mud-snow layer accumulation on adaptive cruise control (acc) system radar and thickness measurement of it,” in *2022 Systems of Signals Generating and Processing in the Field of on Board Communications*, pp. 1–5, 2022.

[542] Z. Zhao and C. Wei, “An analysis of the brake performance of radar-based adaptive cruise control during ramp merging on simulation software,” in *2022 7th International Conference on Intelligent Computing and Signal Processing (ICSP)*, pp. 1112–1115, 2022.

[543] B. Wang, Y. Luo, Z. Zhong, and K. Li, “Robust non-fragile fault tolerant control for ensuring the safety of the intended functionality of cooperative adaptive cruise control,” *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–15, 2022.

[544] H. Zhou, A. Zhou, T. Li, D. Chen, S. Peeta, and J. Laval, “Congestion-mitigating mpc design for adaptive cruise control based on newell’s car following model: History outperforms prediction,” *Transportation Research Part C: Emerging Technologies*, vol. 142, p. 103801, 2022.

[545] Y. Tan and K. Zhang, “Real-time distributed cooperative adaptive cruise control model considering time delays and actuator lag,” *Transportation Research Record*, vol. 0, no. 0, p. 03611981221091762, 0.

[546] E. Kim, “Mimo fmcw radar with doppler-insensitive polyphase codes,” *Remote Sensing*, vol. 14, no. 11, 2022.

[547] S. Lim, J. Jung, J. Kim, S.-C. Kim, and J. Choi, “Enhanced velocity estimation based on joint doppler frequency and range rate measurements,” in *2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 217–221, 2022.

[548] C. Pan, A. Huang, L. Chen, Y. Cai, L. Chen, J. Liang, and W. Zhou, “A review of the development trend of adaptive cruise control for ecological driving,” *Proceedings of the Institution of Mechanical Engineers, Part D: Journal of Automobile Engineering*, vol. 236, no. 9, pp. 1931–1948, 2022.

[549] A. Saffari, S.-H. Zahiri, and M. Khishe, “Automatic recognition of sonar targets using feature selection in micro-doppler signature,” *Defence Technology*, 2022.

[550] C. Flores, P. Merdrignac, R. de Charette, F. Navas, V. Milanés, and F. Nashashibi, “A cooperative car-following/emergency braking system with prediction-based pedestrian avoidance capabilities,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 5, pp. 1837–1846, 2018.

[551] D. Khablov, “Application of super-high frequency doppler displacement sensors in an anti-lock braking system,” *Measurement Techniques*, vol. 64, no. 2, pp. 124–130, 2021.

[552] O. J. Woodman, “An introduction to inertial navigation,” Tech. Rep. UCAM-CL-TR-696, University of Cambridge, Computer Laboratory, August 2007.

[553] N. M. Barbour, “Inertial navigation sensors,” tech. rep., Charles Stark Draper Lab Inc Cambridge Ma, 2010.

[554] X. Wang, J. Wu, T. Xu, and W. Wang, “Analysis and verification of rotation modulation effects on inertial navigation system based on mems sensors,” *Journal of Navigation*, vol. 66, no. 5, p. 751–772, 2013.

[555] K.-P.-H. Thai, O. Rabaste, J. Bosse, D. Poullin, I. Hinostroza, T. Letertre, and T. Chonavel, “Around-the-corner radar: Detection and localization of a target in non-line of sight,” in *2017 IEEE Radar Conference (RadarConf)*, pp. 0842–0847, 2017.

[556] L. De Floriani, P. Marzano, and E. Puppo, “Line-of-sight communication on terrain models,” *International journal of geographical information systems*, vol. 8, no. 4, pp. 329–342, 1994.

[557] Y. Yang, C. Chen, Y. Jia, G. Cui, and S. Guo, “Non-line-of-sight target detection based on dual-view observation with single-channel uwb radar,” *Remote Sensing*, vol. 14, no. 18, p. 4532, 2022.

[558] E. R. Matera, A. Garcia-Pena, O. Julien, C. Milner, and B. Ekambi, “Characterization of line-of-sight and non-line-of-sight pseudorange multipath errors in urban environment for gps and galileo,” in *Proceedings of the 2019 International Technical Meeting of The Institute of Navigation*, pp. 177–196, 2019.

[559] J. Brownjohn, P. Moyo, C. Rizos, and S. Tjin, “Practical issues in using novel sensors in shm of civil infrastructure: problems and solutions in implementation of gps and fibre optic sensors,” 2003.

[560] B. Zhang, J. Ou, Y. Yuan, and Z. Li, “Extraction of line-of-sight ionospheric observables from gps data using precise point positioning,” *Science China Earth Sciences*, vol. 55, no. 11, pp. 1919–1928, 2012.

[561] F. S. Egner, Y. Wang, T. Willems, M. Kirchner, B. Pluymers, W. Desmet, J. Palandri, B. Reff, and F. Wolf-Monheim, “High-speed camera based experimental modal analysis for dynamic testing of an automotive coil spring,” *SAE International Journal of Advances and Current Practices in Mobility*, vol. 4, no. 1, pp. 278–288, 2022.

[562] A. Ometov, V. Shubina, L. Klus, J. Skibińska, S. Saafi, P. Pascacio, L. Flueratoru, D. Q. Gaibor, N. Chukhno, O. Chukhno, *et al.*, "A survey on wearable technology: History, state-of-the-art and current challenges," *Computer Networks*, vol. 193, p. 108074, 2021.

[563] R. M. Paradina and Y. T. Prasetyo, "Particle scrap reduction of an automotive camera product by lean six sigma dmaic approach," in *2021 IEEE 8th International Conference on Industrial Engineering and Applications (ICIEA)*, pp. 384–389, 2021.

[564] S. Alexiou, G. Deligiannakis, A. Pallikarakis, I. Papanikolaou, E. Psomiadis, and K. Reicherter, "Comparing high accuracy t-lidar and uav-sfm derived point clouds for geomorphological change detection," *ISPRS International Journal of Geo-Information*, vol. 10, no. 6, p. 367, 2021.

[565] O. Kilani, M. Gouda, J. Weiß, and K. El-Basyouny, "Safety assessment of urban intersection sight distance using mobile lidar data," *Sustainability*, vol. 13, no. 16, p. 9259, 2021.

[566] N. Levanon and E. Mozeson, *Radar signals*. John Wiley & Sons, 2004.

[567] M. A. Richards, J. Scheer, W. A. Holm, and W. L. Melvin, *Principles of modern radar*, vol. 1. Citeseer, 2010.

[568] A. Pinker and C. Smith, "Vulnerability of the gps signal to jamming," *GPS Solutions*, vol. 3, no. 2, pp. 19–27, 1999.

[569] A. Pinker, D. Walker, and C. Smith, "Jamming the gps signal," in *Proceedings of the 55th Annual Meeting of The Institute of Navigation (1999)*, pp. 829–837, 1999.

[570] M. Oliver, H. Badland, S. Mavoa, M. J. Duncan, and S. Duncan, "Combining gps, gis, and accelerometry: methodological issues in the assessment of location and intensity of travel behaviors," *Journal of Physical Activity and Health*, vol. 7, no. 1, pp. 102–108, 2010.

[571] J. D. Klett, "Stable analytical inversion solution for processing lidar returns," *Applied optics*, vol. 20, no. 2, pp. 211–220, 1981.

[572] X. Meng, N. Currit, and K. Zhao, "Ground filtering algorithms for airborne lidar data: A review of critical issues," *Remote Sensing*, vol. 2, no. 3, pp. 833–860, 2010.

[573] R. Halterman and M. Bruch, "Velodyne hdl-64e lidar for unmanned surface vehicle obstacle detection," in *Unmanned Systems Technology XII*, vol. 7692, pp. 123–130, SPIE, 2010.

[574] D. Puccinelli and M. Haenggi, "Wireless sensor networks: applications and challenges of ubiquitous sensing," *IEEE Circuits and systems magazine*, vol. 5, no. 3, pp. 19–31, 2005.

[575] M. Holder, P. Rosenberger, H. Winner, T. D'hondt, V. P. Makkapati, M. Maier, H. Schreiber, Z. Magosi, Z. Slavik, O. Bringmann, *et al.*, "Measurements revealing challenges in radar sensor modeling for virtual validation of autonomous driving," in *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, pp. 2616–2622, IEEE, 2018.

[576] S. Sen and A. Nehorai, "Adaptive ofdm radar for target detection in multipath scenarios," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 78–90, 2010.

[577] S. Wilson and B. Carlson, "Radar detection in multipath," *IEE Proceedings-Radar, Sonar and Navigation*, vol. 146, no. 1, pp. 45–54, 1999.

[578] M. Leigsnering, F. Ahmad, M. Amin, and A. Zoubir, "Multipath exploitation in through-the-wall radar imaging using sparse reconstruction," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 50, no. 2, pp. 920–939, 2014.

[579] K. M. Larson, E. E. Small, E. Gutmann, A. Bilich, P. Axelrad, and J. Braun, "Using gps multipath to measure soil moisture fluctuations: initial results," *GPS solutions*, vol. 12, no. 3, pp. 173–177, 2008.

[580] T. Kijewski-Correa and M. Kochly, "Monitoring the wind-induced response of tall buildings: Gps performance and the issue of multipath effects," *Journal of Wind Engineering and Industrial Aerodynamics*, vol. 95, no. 9-11, pp. 1176–1198, 2007.

[581] V. U. Zavorotny, K. M. Larson, J. J. Braun, E. E. Small, E. D. Gutmann, and A. L. Bilich, "A physical model for gps multipath caused by land reflections: Toward bare soil moisture retrievals," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 3, no. 1, pp. 100–110, 2009.

[582] B. M. Hannah, *Modelling and simulation of GPS multipath propagation*. PhD thesis, Queensland University of Technology, 2001.

[583] J.-K. Choi, H. N. Nguyen, T. H. Nguyen, H. Cho, H.-K. Choi, S.-G. Park, *et al.*, "A time-domain estimation method of rapidly time-varying channels for ofdm-based lte-r systems," *Digital Communications and Networks*, vol. 5, no. 2, pp. 94–101, 2019.

[584] D. Bharadia and S. Katti, "Fastforward: Fast and constructive full duplex relays," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 4, pp. 199–210, 2014.

[585] V. Venkataramanan and S. Lakshmi, "Hardware co simulation of lte physical layer for mobile network applications," *Future Generation Computer Systems*, vol. 99, pp. 124–133, 2019.

[586] T. Ali-Yahiya, "Lte phyiscal layer," in *Understanding LTE and its Performance*, pp. 55–73, Springer, 2011.

[587] D. Lefloch, R. Nair, F. Lenzen, H. Schäfer, L. Streeter, M. J. Cree, R. Koch, and A. Kolb, "Technical foundation and calibration methods for time-of-flight cameras," in *Time-of-Flight and Depth Imaging. Sensors, Algorithms, and Applications*, pp. 3–24, Springer, 2013.

[588] A. Kadambi, R. Whyte, A. Bhandari, L. Streeter, C. Barsi, A. Dorrington, and R. Raskar, "Coded time of flight cameras: sparse deconvolution to address multipath interference and recover time profiles," *ACM Transactions on Graphics (ToG)*, vol. 32, no. 6, pp. 1–10, 2013.

[589] S. Fuchs, M. Suppa, and O. Hellwich, "Compensation for multipath in tof camera measurements supported by photometric calibration and environment integration," in *International Conference on Computer Vision Systems*, pp. 31–41, Springer, 2013.

[590] D. Jiménez, D. Pizarro, M. Mazo, and S. Palazuelos, "Modeling and correction of multipath interference in time of flight cameras," *Image and Vision Computing*, vol. 32, no. 1, pp. 1–13, 2014.

[591] J. P. Godbaz, A. A. Dorrington, and M. J. Cree, "Understanding and ameliorating mixed pixels and multipath interference in amcw lidar," *TOF Range-Imaging Cameras*, pp. 91–116, 2013.

[592] K. Ali, X. Chen, F. Dovis, D. De Castro, and A. J. Fernández, "Multipath estimation in urban environments from joint gnss receivers and lidar sensors," *Sensors*, vol. 12, no. 11, pp. 14592–14603, 2012.

[593] A. Turpin, V. Kapitany, J. Radford, D. Rovelli, K. Mitchell, A. Lyons, I. Starshynov, and D. Faccio, "3d imaging from multipath temporal echoes," *Physical Review Letters*, vol. 126, no. 17, p. 174301, 2021.

[594] S. Sen, J. Lee, K.-H. Kim, and P. Congdon, "Avoiding multipath to revive inbuilding wifi localization," in *Proceeding of the 11th annual international conference on Mobile systems, applications, and services*, pp. 249–262, 2013.

[595] E. Soltanaghaei, A. Kalyanaraman, and K. Whitehouse, "Multipath triangulation: Decimeter-level wifi localization and orientation with a single unaided receiver," in *Proceedings of the 16th annual international conference on mobile systems, applications, and services*, pp. 376–388, 2018.

[596] F. Liu, J. Liu, Y. Yin, W. Wang, D. Hu, P. Chen, and Q. Niu, "Survey on wifi-based indoor positioning techniques," *IET communications*, vol. 14, no. 9, pp. 1372–1383, 2020.

[597] N. Gavrilov, N. Karpova, C. Jacobi, and A. Gavrilov, "Morphology of atmospheric refraction index variations at different altitudes from gps/met satellite observations," *Journal of atmospheric and solar-terrestrial physics*, vol. 66, no. 6-9, pp. 427–435, 2004.

[598] S. Schaer, G. Beutler, M. Rothacher, E. Brockmann, A. Wiget, and U. Wild, “The impact of the atmosphere and other systematic errors on permanent gps networks,” in *Geodesy Beyond 2000*, pp. 373–380, Springer, 2000.

[599] G. A. Hajj, E. Kursinski, L. Romans, W. Bertiger, and S. Leroy, “A technical description of atmospheric sounding by gps occultation,” *Journal of Atmospheric and Solar-Terrestrial Physics*, vol. 64, no. 4, pp. 451–469, 2002.

[600] Q. Lei, L. Lei, and W. Zemin, “An tropospheric delay model for gps net rtk,” in *2010 Second International Conference on Information Technology and Computer Science*, pp. 98–101, IEEE, 2010.

[601] M. I. Skolnik, “Introduction to radar,” *Radar handbook*, vol. 2, p. 21, 1962.

[602] K. Qian, S. Zhu, X. Zhang, and L. E. Li, “Robust multimodal vehicle detection in foggy weather using complementary lidar and radar signals,” in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 444–453, 2021.

[603] M. Skolnik, “An introduction and overview of radar,” *Radar Handbook*, vol. 3, pp. 1–1, 2008.

[604] R. H. Rasshofer, M. Spies, and H. Spies, “Influences of weather phenomena on automotive laser radar systems,” *Advances in Radio Science*, vol. 9, no. B. 2, pp. 49–60, 2011.

[605] P. Kintner, M. Psiaki, T. Humphreys, *et al.*, “A beginner’s guide to space weather and gps,” *Lectnre notes, Updated Fehruary*, vol. 21, 2008.

[606] I. Srivani, G. S. V. Prasad, and D. V. Ratnam, “A deep learning-based approach to forecast ionospheric delays for gps signals,” *IEEE Geoscience and Remote Sensing Letters*, vol. 16, no. 8, pp. 1180–1184, 2019.

[607] A. Coster and A. Komjathy, “Space weather and the global positioning system,” *Space Weather*, vol. 6, no. 6, 2008.

[608] P. Kintner, H. Kil, T. Beach, and E. de Paula, “Fading timescales associated with GPS signals and potential consequences,” *Radio Science*, vol. 36, no. 4, pp. 731–743, 2001.

[609] S. P. Thiagarajah, S. Pillay, S. Darmaraju, R. Subramanian, and M. F. M. Fung, “The effect of rain attenuation on s-band terrestrial links,” in *2013 IEEE Symposium on Wireless Technology & Applications (ISWTA)*, pp. 192–197, IEEE, 2013.

[610] S. G. Narasimhan and S. K. Nayar, “Removing weather effects from monochrome images,” in *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. CVPR 2001*, vol. 2, pp. II–II, IEEE, 2001.

[611] R. Heinzler, P. Schindler, J. Seekircher, W. Ritter, and W. Stork, “Weather influence and classification with automotive lidar sensors,” in *2019 IEEE intelligent vehicles symposium (IV)*, pp. 1527–1534, IEEE, 2019.

[612] Y. Golovachev, A. Etinger, G. A. Pinhasi, and Y. Pinhasi, “Millimeter wave high resolution radar accuracy in fog conditions—theory and experimental verification,” *Sensors*, vol. 18, no. 7, 2018.

[613] N. Balal, G. A. Pinhasi, and Y. Pinhasi, “Atmospheric and fog effects on ultra-wide band radar operating at extremely high frequencies,” *Sensors*, vol. 16, no. 5, 2016.

[614] E. G. Wærsted, M. Haeffelin, J.-C. Dupont, J. Delanoë, and P. Dubuisson, “Radiation in fog: quantification of the impact on fog liquid water based on ground-based remote sensing,” *Atmospheric Chemistry and Physics*, vol. 17, no. 17, pp. 10811–10835, 2017.

[615] F. S. Solheim, J. Vivekanandan, R. H. Ware, and C. Rocken, “Propagation delays induced in gps signals by dry air, water vapor, hydrometeors, and other particulates,” *Journal of Geophysical Research: Atmospheres*, vol. 104, no. D8, pp. 9663–9670, 1999.

[616] S. Zang, M. Ding, D. Smith, P. Tyler, T. Rakotoarivelo, and M. A. Kaafar, “The impact of adverse weather conditions on autonomous vehicles: How rain, snow, fog, and hail affect the performance of a self-driving car,” *IEEE Vehicular Technology Magazine*, vol. 14, no. 2, pp. 103–111, 2019.

[617] D. H. S. Lima, A. L. L. Aquino, and M. Curado, “A review of mobility prediction models applied in cloud/fog environments,” in *Euro-Par 2018: Parallel Processing Workshops* (G. Mencagli, D. B. Heras, V. Cardellini, E. Casalicchio, E. Jeannot, F. Wolf, A. Salis, C. Schifanella, R. R. Manumachu, L. Ricci, M. Beccuti, L. Antonelli, J. D. Garcia Sanchez, and S. L. Scott, eds.), (Cham), pp. 263–274, Springer International Publishing, 2019.

[618] S. Singh and J. Singh, *Location Driven Edge Assisted Device and Solutions for Intelligent Transportation*, ch. 7, pp. 123–147. John Wiley & Sons, Ltd, 2020.

[619] R. M. Pierce, J. Ramaprasad, and E. C. Eisenberg, “Optical attenuation in fog and clouds,” in *Optical Wireless Communications IV* (E. J. Korevaar, ed.), vol. 4530, pp. 58 – 71, International Society for Optics and Photonics, SPIE, 2001.

[620] R. Gallen, A. Cord, N. Hautière, and D. Aubert, “Towards night fog detection through use of in-vehicle multipurpose cameras,” in *2011 IEEE Intelligent Vehicles Symposium (IV)*, pp. 399–404, 2011.

[621] L. R. Bissonnette and D. L. Hutt, “Lidar remote sensing of cloud and fog properties,” in *Air Pollution and Visibility Measurements* (P. Fabian, V. Klein, M. Tacke, K. Weber, and C. Werner, eds.), vol. 2506, pp. 512 – 523, International Society for Optics and Photonics, SPIE, 1995.

[622] A. Ronen, E. Agassi, and O. Yaron, “Sensing with polarized lidar in degraded visibility conditions due to fog and low clouds,” *Sensors*, vol. 21, no. 7, 2021.

[623] K. Qian, S. Zhu, X. Zhang, and L. E. Li, “Robust multimodal vehicle detection in foggy weather using complementary lidar and radar signals,” in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 444–453, June 2021.

[624] D. Rupprecht, K. Kohls, T. Holz, and C. Pöpper, “Call me maybe: Eavesdropping encrypted LTE calls with ReVoLTE,” in *29th USENIX Security Symposium (USENIX Security 20)*, pp. 73–88, USENIX Association, August 2020.

[625] C. Tata and M. Kadoch, “Secure multipath routing algorithm for device-to-device communications for public safety over lte heterogeneous networks,” in *2015 3rd International Conference on Future Internet of Things and Cloud*, pp. 212–217, 2015.

[626] H. Fang, L. Xu, Y. Zou, X. Wang, and K.-K. R. Choo, “Three-stage stackelberg game for defending against full-duplex active eavesdropping attacks in cooperative communication,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 10788–10799, 2018.

[627] H. Xia and J. C. Brustoloni, “Hardening web browsers against man-in-the-middle and eavesdropping attacks,” in *Proceedings of the 14th International Conference on World Wide Web*, WWW ’05, (New York, NY, USA), p. 489–498, Association for Computing Machinery, 2005.

[628] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: Technical challenges, recent advances, and future trends,” *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[629] M. Alyami, I. Alharbi, C. Zou, Y. Solihin, and K. Ackerman, “Wifi-based iot devices profiling attack based on eavesdropping of encrypted wifi traffic,” in *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, pp. 385–392, 2022.

[630] T. Fei and W. Wang, “Lte is vulnerable: Implementing identity spoofing and denial-of-service attacks in lte networks,” in *2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, 2019.

[631] R. Ghannam, F. Sharevski, and A. Chung, “User-targeted denial-of-service attacks in lte mobile networks,” in *2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 1–8, 2018.

[632] M. R. Dey, M. Patra, and P. Mishra, “Real-time detection and localization of denial-of-service attacks in heterogeneous vehicular networks,” in *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 1434–1439, 2021.

[633] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, “Denial of service attacks in wireless networks: The case of jammers,” *IEEE Communications Surveys & Tutorials*, vol. 13, no. 2, pp. 245–257, 2011.

[634] K. Bicakci and B. Tavli, “Denial-of-service attacks and countermeasures in ieee 802.11 wireless networks,” *Computer Standards & Interfaces*, vol. 31, no. 5, pp. 931–941, 2009. Specification, Standards and Information Management for Distributed Systems.

[635] G. Carl, G. Kesidis, R. Brooks, and S. Rai, “Denial-of-service attack-detection techniques,” *IEEE Internet Computing*, vol. 10, no. 1, pp. 82–89, 2006.

[636] A. Hussain, J. Heidemann, and C. Papadopoulos, “A framework for classifying denial of service attacks,” in *Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, SIGCOMM ’03, (New York, NY, USA), p. 99–110, Association for Computing Machinery, 2003.

[637] D. S. Reddy, V. Bapuji, A. Govardhan, and S. S. V. N. Sarma, “Sybil attack detection technique using session key certificate in vehicular ad hoc networks,” in *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*, pp. 1–5, 2017.

[638] J. Grover, D. Kumar, M. Sargurunathan, M. S. Gaur, and V. Laxmi, “Performance evaluation and detection of sybil attacks in vehicular ad-hoc networks,” in *Recent Trends in Network Security and Applications* (N. Meghanathan, S. Boumerdassi, N. Chaki, and D. Nagamalai, eds.), (Berlin, Heidelberg), pp. 473–482, Springer Berlin Heidelberg, 2010.

[639] Y. Yao, B. Xiao, G. Wu, X. Liu, Z. Yu, K. Zhang, and X. Zhou, “Voiceprint: A novel sybil attack detection method based on rssi for vanets,” in *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 591–602, 2017.

[640] H. Hamed, A. Keshavarz-Haddad, and S. G. Haghighi, “Sybil attack detection in urban vanets based on rsu support,” in *Electrical Engineering (ICEE), Iranian Conference on*, pp. 602–606, 2018.

[641] Y. Yao, B. Xiao, G. Wu, X. Liu, Z. Yu, K. Zhang, and X. Zhou, “Multi-channel based sybil attack detection in vehicular ad hoc networks using rssi,” *IEEE Transactions on Mobile Computing*, vol. 18, no. 2, pp. 362–375, 2019.

[642] X. Wang, L. Liu, L. Zhu, and T. Tang, “Joint security and qos provisioning in train-centric cbtc systems under sybil attacks,” *IEEE Access*, vol. 7, pp. 91169–91182, 2019.

[643] A. Vasudeva and M. Sood, “On the vulnerability of the mobile ad hoc network to transmission power controlled sybil attack: Adopting the mobility-based clustering,” *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 9, pp. 7025–7044, 2022.

[644] J. Yang, Y. Chen, and W. Trappe, “Detecting sybil attacks inwireless and sensor networks using cluster analysis,” in *2008 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, pp. 834–839, 2008.

[645] K. Zhang, X. Liang, R. Lu, and X. Shen, “Sybil attacks and their defenses in the internet of things,” *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372–383, 2014.

[646] A. Tsiota, D. Xenakis, N. Passas, and L. Merakos, “On jamming and black hole attacks in heterogeneous wireless networks,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 10761–10774, 2019.

[647] A. Kumar, V. Varadarajan, A. Kumar, P. Dadheech, S. S. Choudhary, V. A. Kumar, B. Panigrahi, and K. C. Veluvolu, “Black hole attack detection in vehicular ad-hoc network using secure aodv routing algorithm,” *Microprocessors and Microsystems*, vol. 80, p. 103352, 2021.

[648] F. Al-Turjman and J. P. Lemayian, “Intelligence, security, and vehicular sensor networks in internet of things (iot)-enabled smart-cities: An overview,” *Computers & Electrical Engineering*, vol. 87, p. 106776, 2020.

[649] R. Ranjan, N. K. Singh, and A. Singh, “Security issues of black hole attacks in manet,” in *International Conference on Computing, Communication & Automation*, pp. 452–457, 2015.

[650] P. Golchha and H. K. Pati, "A survey on black hole attack in manet using aodv," in *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, pp. 361–365, 2018.

[651] S. Cohen, T. Gluck, Y. Elovici, and A. Shabtai, "Security analysis of radar systems," in *Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy*, pp. 3–14, 2019.

[652] A. Costin and A. Francillon, "Ghost in the Air(Traffic): on insecurity of ADS-B protocol and practical attacks on ADS-B devices," in *Blackhat*, July 2012.

[653] L. Hu, X. Zhou, X. Zhang, F. Wang, Q. Li, and W. Wu, "A review on key challenges in intelligent vehicles: Safety and driver-oriented features," *IET Intelligent Transport Systems*, vol. 15, no. 9, pp. 1093–1105, 2021.

[654] G. R. Andreica, L. Bozga, D. Zinca, and V. Dobrota, "Denial of service and man-in-the-middle attacks against iot devices in a gps-based monitoring software for intelligent transportation systems," in *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pp. 1–4, IEEE, 2020.

[655] Z. El-Rewini, K. Sadatsharan, N. Sugunaraj, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity attacks in vehicular sensors," *IEEE Sensors Journal*, vol. 20, no. 22, pp. 13752–13767, 2020.

[656] G. B. Gaggero, A. Fausto, F. Patrone, and M. Marchese, "A framework for network security verification of automated vehicles in the agricultural domain," in *2022 26th International Conference Electronics*, pp. 1–5, IEEE, 2022.

[657] T. Fei and W. Wang, "Lte is vulnerable: implementing identity spoofing and denial-of-service attacks in lte networks," in *2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, IEEE, 2019.

[658] A. H. El-Sakka, S. Shaaban, and K. H. Moussa, "Double evolved packet system authentication and key agreement protocol based on elliptic curve for 4g (lte) networks," in *2021 International Telecommunications Conference (ITC-Egypt)*, pp. 1–5, IEEE, 2021.

[659] R. Selvaraj, V. M. Kuthadi, S. Baskar, P. M. Shakeel, and A. Ranjan, "Creating security modelling framework analysing in internet of things using ec-gsm-iot," *Arabian Journal for Science and Engineering*, pp. 1–13, 2021.

[660] Y. Meng, J. Li, H. Zhu, X. Liang, Y. Liu, and N. Ruan, "Revealing your mobile password via wifi signals: Attacks and countermeasures," *IEEE Transactions on Mobile Computing*, vol. 19, no. 2, pp. 432–449, 2019.

[661] H. M. Rouzbahani, H. Karimipour, E. Fraser, A. Dehghantanha, E. Duncan, A. Green, and C. Russell, "Communication layer security in smart farming: A survey on wireless technologies," *arXiv preprint arXiv:2203.06013*, 2022.

[662] J. Cathalo, F. Koeune, and J.-J. Quisquater, "A new type of timing attack: Application to gps," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 291–303, Springer, 2003.

[663] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley, "GPS software attacks," in *Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 450–461, ACM, 2012.

[664] C. Bonebrake and L. R. O'Neil, "Attacks on gps time reliability," *IEEE Security & Privacy*, vol. 12, no. 3, pp. 82–84, 2014.

[665] S. Bae, M. Son, D. Kim, C. Park, J. Lee, S. Son, and Y. Kim, "Watching the watchers: Practical video identification attack in {LTE} networks," in *31st USENIX Security Symposium (USENIX Security 22)*, pp. 1307–1324, 2022.

[666] S. Bhattarai, S. Rook, L. Ge, S. Wei, W. Yu, and X. Fu, "On simulation studies of cyber attacks against lte networks," in *2014 23rd International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–8, IEEE, 2014.

[667] M. S. Lund, O. S. Hareide, and Ø. Jøsok, "An attack on an integrated navigation system," 2018.

[668] F. Ahmad, A. Adnane, V. N. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies," *Sensors*, vol. 18, no. 11, p. 4040, 2018.

[669] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE communications surveys & tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.

[670] P. Kapoor, A. Vora, and K.-D. Kang, "Detecting and mitigating spoofing attack against an automotive radar," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, pp. 1–6, IEEE, 2018.

[671] K. C. Zeng, Y. Shu, S. Liu, Y. Dou, and Y. Yang, "A practical gps location spoofing attack in road navigation scenario," in *Proceedings of the 18th international workshop on mobile computing systems and applications*, pp. 85–90, 2017.

[672] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "Gps vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, vol. 2012, 2012.

[673] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "Lte/lte-a jamming, spoofing, and sniffing: threat assessment and mitigation," *IEEE Communications Magazine*, vol. 54, no. 4, pp. 54–61, 2016.

[674] D. Nassi, R. Ben-Netanel, Y. Elovici, and B. Nassi, "Mobilbye: attacking adas with camera spoofing," *arXiv preprint arXiv:1906.09765*, 2019.

[675] Z. Jiang, K. Zhao, R. Li, J. Zhao, and J. Du, "Phyalert: identity spoofing attack detection and prevention for a wireless edge network," *Journal of Cloud Computing*, vol. 9, no. 1, pp. 1–13, 2020.

[676] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in wsns," *IEEE communications surveys & tutorials*, vol. 11, no. 4, pp. 42–56, 2009.

[677] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, 2022.

[678] M. P. Arthur, "Detecting signal spoofing and jamming attacks in uav networks using a lightweight ids," in *2019 international conference on computer, information and telecommunication systems (CITS)*, pp. 1–5, IEEE, 2019.

[679] R. P. Jover, J. Lackey, and A. Raghavan, "Enhancing the security of lte networks against jamming attacks," *EURASIP Journal on Information Security*, vol. 2014, no. 1, pp. 1–14, 2014.

[680] S. Djuraev, J.-G. Choi, K.-S. Sohn, and S. Y. Nam, "Channel hopping scheme to mitigate jamming attacks in wireless lans," *EURASIP Journal on Wireless Communications and Networking*, vol. 2017, no. 1, pp. 1–12, 2017.

[681] E. Yeh, J. Choi, N. G. Prelcic, C. Bhat, and R. W. Heath Jr, "Security in automotive radar and vehicular networks," *Microwave Journal*, 2017.

[682] R. Changalvala, B. Fedoruk, and H. Malik, "Radar data integrity verification using 2d qim-based data hiding," *Sensors*, vol. 20, no. 19, p. 5530, 2020.

[683] D. Luong and B. Balaji, "Quantum radar, quantum networks, not-so-quantum hackers," in *Signal Processing, Sensor/Information Fusion, and Target Recognition XXVIII*, vol. 11018, pp. 418–423, SPIE, 2019.

[684] J. Pan, “Physical integrity attack detection of surveillance camera with deep learning based video frame interpolation,” in *2019 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*, pp. 79–85, IEEE, 2019.

[685] K. M. Ahmad Yousef, A. AlMajali, S. A. Ghalyon, W. Dweik, and B. J. Mohd, “Analyzing cyber-physical threats on robotic platforms,” *Sensors*, vol. 18, no. 5, p. 1643, 2018.

[686] C. Yang, L. Feng, H. Zhang, S. He, and Z. Shi, “A novel data fusion algorithm to combat false data injection attacks in networked radar systems,” *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 125–136, 2018.

[687] W. Jeon, Z. Xie, A. Zemouche, and R. Rajamani, “Simultaneous cyber-attack detection and radar sensor health monitoring in connected acc vehicles,” *IEEE Sensors Journal*, vol. 21, no. 14, pp. 15741–15752, 2020.

[688] Y. Zhang, J. Wang, and J. Liu, “Attack identification and correction for pmu gps spoofing in unbalanced distribution systems,” *IEEE transactions on smart grid*, vol. 11, no. 1, pp. 762–773, 2019.

[689] S. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, “Lteinspector: A systematic approach for adversarial testing of 4g lte,” in *Network and Distributed Systems Security (NDSS) Symposium 2018*, 2018.

[690] C. You, Z. Hau, and S. Demetriou, “Temporal consistency checks to detect lidar spoofing attacks on autonomous vehicle perception,” in *Proceedings of the 1st Workshop on Security and Privacy for Mobile AI*, pp. 13–18, 2021.

[691] W. Liu, W. He, B. Hu, and C.-H. Chang, “A practical man-in-the-middle attack on deep learning edge device by sparse light strip injection into camera data lane,” in *2022 IEEE 35th International System-on-Chip Conference (SOCC)*, pp. 1–6, IEEE, 2022.

[692] F. J. Aparicio-Navarro, K. G. Kyriakopoulos, and D. J. Parish, “An automatic and self-adaptive multi-layer data fusion system for wifi attack detection,” *International Journal of Internet Technology and Secured Transactions*, 2013.

[693] T. de Riberolles, J. Song, Y. Zou, G. Silvestre, and N. Larrieu, “Characterizing radar network traffic: a first step towards spoofing attack detection,” in *2020 IEEE Aerospace Conference*, pp. 1–8, IEEE, 2020.

[694] M. El-Said, X. Wang, S. Mansour, and A. Kalafut, “Building an impersonation attack and defense testbed for vehicle to vehicle systems,” in *Proceedings of the 22st Annual Conference on Information Technology Education*, pp. 65–66, 2021.

[695] D. Rupprecht, K. Kohls, T. Holz, and C. Pöpper, “Imp4gt: Impersonation attacks in 4g networks.,” in *NDSS*, 2020.

[696] D.-L. Nguyen, S. S. Arora, Y. Wu, and H. Yang, “Adversarial light projection attacks on face recognition systems: A feasibility study,” in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition workshops*, pp. 814–815, 2020.

[697] M. Dibaei, X. Zheng, K. Jiang, R. Abbas, S. Liu, Y. Zhang, Y. Xiang, and S. Yu, “Attacks and defences on intelligent connected vehicles: A survey,” *Digital Communications and Networks*, vol. 6, no. 4, pp. 399–421, 2020.

[698] H. P. D. Nguyen and R. Zoltán, “The security concerns and countermeasures towards v2v and autonomous cars,” in *Proceedings of Sixth International Congress on Information and Communication Technology*, pp. 535–544, Springer, 2022.

[699] M. E. Aminanto and K. Kim, “Detecting impersonation attack in wifi networks using deep learning approach,” in *International workshop on information security applications*, pp. 136–147, Springer, 2016.

[700] J. T. Isaac, S. Zeadally, and J. S. Camara, “Security attacks and solutions for vehicular ad hoc networks,” *IET communications*, vol. 4, no. 7, pp. 894–903, 2010.

[701] S. L. Pais, P. S. Nikshita, S. Priyanka, and U. Tharunya, “Illusion pin: tricking the eye to defeat shoulder surfing attack by using hybrid images,” *Editorial Board*, vol. 9, no. 7, 2020.

[702] M. Hadded, O. Shagdar, and P. Merdrignac, “Augmented perception by v2x cooperation (pac-v2x): Security issues and misbehavior detection solutions,” in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 907–912, 2019.

[703] M. R. Ansari, J.-P. Monteuuis, J. Petit, and C. Chen, “V2x misbehavior and collective perception service: Considerations for standardization,” in *2021 IEEE Conference on Standards for Communications and Networking (CSCN)*, pp. 1–6, 2021.

[704] W. Pi, P. Yang, D. Duan, C. Chen, X. Cheng, L. Yang, and H. Li, “Malicious user detection for cooperative mobility tracking in autonomous driving,” *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4922–4936, 2020.

[705] B. Sheehan, F. Murphy, M. Mullins, and C. Ryan, “Connected and autonomous vehicles: A cyber-risk classification framework,” *Transportation research part A: policy and practice*, vol. 124, pp. 523–536, 2019.

[706] C. Premebida, J. Carreira, J. Batista, and U. Nunes, “Pedestrian detection combining RGB and dense LIDAR data,” pp. 4112–4117, IEEE, 2014.

[707] G. Melotti, C. Premebida, and N. Gonçalves, “Multimodal deep-learning for object recognition combining camera and LIDAR data,” pp. 177–182, IEEE, 2020.

[708] M. M. Islam, A. A. R. Newaz, and A. Karimoddini, “A pedestrian detection and tracking framework for autonomous cars: efficient fusion of camera and LiDAR data,” *arXiv preprint arXiv:2108.12375*, 2021.

[709] S. Turner, M. Martin, G. Griffin, M. Le, S. Das, B. Dadashova, and X. Li, “Exploring crowdsourced monitoring data for safety,” final research report, Safety through Disruption (Safe-D) National University Transportation Center, 2020.

[710] X. Zheng, W. Chen, P. Wang, D. Shen, S. Chen, X. Wang, Q. Zhang, and L. Yang, “Big data for social transportation,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, pp. 620–630, March 2016. Conference Name: IEEE Transactions on Intelligent Transportation Systems.

[711] K. Lee and I. N. Sener, “Emerging data mining for pedestrian and bicyclist monitoring: A literature review report,” *Safety through Disruption (Safe-D) National University Transportation Center (UTC) Program*, 2017.

[712] A. Smith, “Crowdsourcing pedestrian and cyclist activity data,” tech. rep., University of North Carolina, Chapel Hill Highway Safety Research Center, Pedestrian and Bicycle Information, 2015.

[713] A. Misra, A. Gooze, K. Watkins, M. Asad, and C. A. Le Dantec, “Crowdsourcing and its application to transportation data collection and management,” *Transportation Research Record*, vol. 2414, pp. 1–8, January 2014. Publisher: SAGE Publications Inc.

[714] X. Wang, X. Zheng, Q. Zhang, T. Wang, and D. Shen, “Crowdsourcing in ITS: the state of the work and the networking,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, pp. 1596–1605, June 2016. Conference Name: IEEE Transactions on Intelligent Transportation Systems.

[715] S. Parkinson, P. Ward, K. Wilson, and J. Miller, “Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges,” *IEEE Transactions on Intelligent Transportation Systems (ITS)*, vol. 18, no. 11, pp. 2898–2915, 2017.

[716] X. Sun, F. R. Yu, and P. Zhang, “A survey on cyber-security of connected and autonomous vehicles (cavs),” *IEEE Transactions on Intelligent Transportation Systems*, 2021.

[717] M. Kim, D. Lee, J. Ahn, M. Kim, and J. Park, “Model predictive control method for autonomous vehicles using time-varying and non-uniformly spaced horizon,” *IEEE Access*, vol. 9, pp. 86475–86487, 2021.

[718] Q. Luo, Y. Cao, J. Liu, and A. Benslimane, “Localization and navigation in autonomous driving: Threats and countermeasures,” *IEEE Wireless Communications*, vol. 26, no. 4, pp. 38–45, 2019.

[719] K. H. Janstrup, “Road safety annual report 2017,” *Technical University of Denmark: Lyngby, Denmark*, 2017.

[720] P. Sewalkar, S. Krug, and J. Seitz, “Towards 802.11 p-based vehicle-to-pedestrian communication for crash prevention systems,” in *2017 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pp. 404–409, IEEE, 2017.

[721] A. Rostami, B. Cheng, H. Lu, J. B. Kenney, and M. Gruteser, “Performance and channel load evaluation for contextual pedestrian-to-vehicle transmissions,” in *Proceedings of the First ACM International Workshop on Smart, Autonomous, and Connected Vehicular Systems and Services*, pp. 22–29, 2016.

[722] X. Wu, R. Miucic, S. Yang, S. Al-Stouhi, J. Misener, S. Bai, and W.-h. Chan, “Cars talk to phones: A dsrc based vehicle-pedestrian safety system,” in *2014 IEEE 80th Vehicular Technology Conference (VTC2014-Fall)*, pp. 1–7, IEEE, 2014.

[723] J. J. Anaya, P. Merdrignac, O. Shagdar, F. Nashashibi, and J. E. Naranjo, “Vehicle to pedestrian communications for protection of vulnerable road users,” in *2014 IEEE Intelligent Vehicles Symposium Proceedings*, pp. 1037–1042, IEEE, 2014.

[724] S. Miura, L.-T. Hsu, F. Chen, and S. Kamijo, “Gps error correction with pseudorange evaluation using three-dimensional maps,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 3104–3115, 2015.

[725] E. Adamey, G. Ozbilgin, and U. Ozguner, “Collaborative vehicle tracking in mixed-traffic environments: Scaled-down tests using simville,” tech. rep., SAE Technical Paper, 2015.

[726] S. Moore, “Superaccurate gps chips coming to smartphones in 2018 (2017),” *URL https://spectrum. ieee. org/tech-talk/semiconductors/design/superaccurate-gps-chips-coming-to-smartphones-in-2018.(Accessed 18 November 2017)*.

[727] S. Jwa, Ü. Ozguner, and Z. Tang, “Information-theoretic data registration for uav-based sensing,” *IEEE Transactions on intelligent transportation systems*, vol. 9, no. 1, pp. 5–15, 2008.

[728] E. Adamey and U. Ozguner, “Cooperative multitarget tracking and surveillance with mobile sensing agents: A decentralized approach,” in *2011 14th International IEEE conference on intelligent transportation systems (ITSC)*, pp. 1916–1922, IEEE, 2011.

[729] P. V. Borges, A. Tews, and D. Haddon, “Pedestrian detection in industrial environments: Seeing around corners,” in *2012 IEEE/RSJ International Conference on Intelligent Robots and Systems*, pp. 4231–4232, IEEE, 2012.

[730] S. Y. Gelbal, S. Arslan, H. Wang, B. Aksun-Guvenc, and L. Guvenc, “Elastic band based pedestrian collision avoidance using v2x communication,” in *2017 IEEE Intelligent Vehicles Symposium (IV)*, pp. 270–276, IEEE, 2017.

[731] C. Sugimoto, Y. Nakamura, and T. Hashimoto, “Prototype of pedestrian-to-vehicle communication system for the prevention of pedestrian accidents using both 3g wireless and wlan communication,” in *2008 3rd International Symposium on Wireless Pervasive Computing*, pp. 764–767, IEEE, 2008.

[732] S. Lee and D. Kim, “An energy efficient vehicle to pedestrian communication method for safety applications,” *Wireless Personal Communications*, vol. 86, no. 4, pp. 1845–1856, 2016.

[733] K. David and A. Flach, “Car-2-x and pedestrian safety,” *IEEE Vehicular Technology Magazine*, vol. 5, no. 1, pp. 70–76, 2010.

[734] D. Sattar, A. H. Vasoukolaei, P. Crysdale, and A. Matrawy, “A stride threat model for 5g core slicing,” in *2021 IEEE 4th 5G World Forum (5GWF)*, pp. 247–252, IEEE, 2021.

[735] R. Hasan and R. Hasan, “Towards a threat model and privacy analysis for v2p in 5g networks,” in *2021 IEEE 4th 5G World Forum (5GWF)*, pp. 383–387, IEEE, 2021.

[736] Y. Yan, B. Zhang, J. Zhou, Y. Zhang, and X. Liu, "Real-time localization and mapping utilizing multi-sensor fusion and visual–imu–wheel odometry for agricultural robots in unstructured, dynamic and gps-denied greenhouse environments," *Agronomy*, vol. 12, 8 2022.

[737] L. Marković, M. Kovač, R. Milijas, M. Car, and S. Bogdan, "Error state extended Kalman filter multi-sensor fusion for unmanned aerial vehicle localization in GPS and magnetometer denied indoor environments," pp. 184–190, IEEE, 2022.

[738] J. Shen, J. Y. Won, Z. Chen, and Q. A. Chen, "Drift with Devil: Security of Multi-Sensor Fusion based Localization in High-Level Autonomous Driving under GPS Spoofing," pp. 931–948, 2020.

[739] Y. Gao, S. Liu, M. Atia, and A. Noureldin, "INS/GPS/LiDAR Integrated Navigation System for Urban and Indoor Environments Using Hybrid Scan Matching Algorithm," *Sensors*, vol. 15, no. 9, pp. 23286–23302, 2015.

[740] J. K. Suhr, J. Jang, D. Min, and H. G. Jung, "Sensor Fusion-based Low-Cost Vehicle Localization System for Complex Urban Environments," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 5, pp. 1078–1086, 2016.

[741] Z. Tao, P. Bonnifait, V. Fremont, and J. Ibanez-Guzman, "Mapping and Localization Using GPS, Lane Markings and Proprioceptive Sensors," in *2013 IEEE/RSJ International Conference on Intelligent Robots and Systems*, pp. 406–412, IEEE, 2013.

[742] I. Hwang, S. Kim, Y. Kim, and C. E. Seah, "A survey of fault detection, isolation, and reconfiguration methods," *IEEE Transactions on Control Systems Technology*, vol. 18, pp. 636–653, 5 2010.

[743] G. Wan, X. Yang, R. Cai, H. Li, Y. Zhou, H. Wang, and S. Song, "Robust and Precise Vehicle Localization based on Multi-Sensor Fusion in Diverse City Scenes," in *ICRA*, pp. 4670–4677, IEEE, 2018.

[744] S. Piperakis, D. Kanoulas, N. G. Tsagarakis, and P. Trahanias, "Outlier-Robust State Estimation for Humanoid Robots," in *IROS*, IEEE, 2019.

[745] X. Zuo, P. Geneva, W. Lee, Y. Liu, and G. Huang, "LIC-Fusion: LiDAR-Inertial-Camera Odometry," *arXiv preprint arXiv:1909.04102*, 2019.

[746] X. Zuo, P. Geneva, Y. Yang, W. Ye, Y. Liu, and G. Huang, "Visual-Inertial Localization With Prior LiDAR Map Constraints," *IEEE Robotics and Automation Letters*, vol. 4, no. 4, pp. 3394–3401, 2019.

[747] M. Miiller, F. Steidle, M. J. Schuster, P. Lutz, M. Maier, S. Stoneman, T. Tomic, and W. Stürzl, "Robust Visual-Inertial State Estimation with Multiple Odometries and Efficient Mapping on an MAV with Ultra-Wide FOV Stereo Vision," in *IROS*, pp. 3701–3708, IEEE, 2018.

[748] K. Eckenhoff, P. Geneva, J. Bloecker, and G. Huang, "Multi-Camera Visual-Inertial Navigation with Online Intrinsic and Extrinsic Calibration," in *ICRA*, pp. 3158–3164, IEEE, 2019.

[749] G. D. Arana, M. Joerger, and M. Spenko, "Efficient Integrity Monitoring for KF-based Localization," in *ICRA*, IEEE, 2019.

[750] E. Allak, R. Jung, and S. Weiss, "Covariance Pre-Integration for Delayed Measurements in Multi-Sensor Fusion," in *IROS*, IEEE, 2019.

[751] M. Brossard and S. Bonnabel, "Learning Wheel Odometry and IMU Errors for Localization," in *ICRA*, IEEE, 2019.

[752] N. Gosala, A. Bühler, M. Prajapat, C. Ehmke, M. Gupta, R. Sivanesan, A. Gawel, M. Pfeiffer, M. Bürki, I. Sa, *et al.*, "Redundant Perception and State Estimation for Reliable Autonomous Racing," in *ICRA*, pp. 6561–6567, IEEE, 2019.

[753] Z. Zhang, S. Liu, G. Tsai, H. Hu, C.-C. Chu, and F. Zheng, "Pirvs: An Advanced Visual-Inertial SLAM System with Flexible Sensor Fusion and Hardware Co-design," in *ICRA*, pp. 1–7, IEEE, 2018.

[754] V. T. Pham, V. T. Nguyen, D. T. Chu, and D. T. Tran, "15-state extended kalman filter design for ins/gps navigation system," *Journal of Automation and Control Engineering*, vol. 3, no. 2, 2015.

[755] Y. Wu and J. Zhao, “A Robust and Precise LiDAR-Inertial-GPS Odometry and Mapping Method for Large-Scale Environment,” *IEEE/ASME Transactions on Mechatronics*, vol. 27, pp. 5027–5036, 12 2022.

[756] E. Zhang and N. Masoud, “Increasing GPS Localization Accuracy with Reinforcement Learning,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, pp. 2615–2626, 5 2021.

[757] G. Rigatos and S. Tzafestas, “Extended kalman filtering for fuzzy modelling and multi-sensor fusion,” *Mathematical and computer modelling of dynamical systems*, vol. 13, no. 3, pp. 251–266, 2007.

[758] M. Brossard, S. Bonnabel, and A. Barrau, “Unscented Kalman Filter on Lie Groups for Visual Inertial Odometry,” in *IROS*, IEEE, 2018.

[759] F. Poggenhans, N. O. Salscheider, and C. Stiller, “Precise Localization in High-definition Road Maps for Urban Regions,” in *IROS*, pp. 2167–2174, IEEE, 2018.

[760] S. Arnold and L. Medagoda, “Robust Model-Aided Inertial Localization for Autonomous Underwater Vehicles,” in *ICRA*, IEEE, 2018.

[761] C. Smaili, M. E. El Najjar, and F. Charpillet, “Multi-sensor fusion method using dynamic bayesian network for precise vehicle localization and road matching,” in *19th IEEE International Conference on Tools with Artificial Intelligence (ICTAI 2007)*, vol. 1, pp. 146–151, IEEE, 2007.

[762] J. Liu and G. Guo, “Vehicle Localization during GPS Outages with Extended Kalman Filter and Deep Learning,” *IEEE Transactions on Instrumentation and Measurement*, vol. 70, 2021.

[763] P. Glavine, O. De Silva, G. Mann, and R. Gosine, “GPS integrated inertial navigation system using Interactive Multiple Model Extended Kalman Filtering,” in *2018 Moratuwa Engineering Research Conference (MERCon)*, pp. 414–419, IEEE, 2018.

[764] K. Jo, K. Chu, and M. Sunwoo, “Gps-bias correction for precise localization of autonomous vehicles,” pp. 636–641, 2013.

[765] D. Zhang, J. Gabaldon, L. Lauderdale, M. Johnson-Roberson, L. J. Miller, K. Barton, and K. A. Shorter, “Localization and Tracking of Uncontrollable Underwater Agents: Particle Filter Based Fusion of On-Body IMUs and Stationary Cameras,” in *ICRA*, IEEE, 2019.

[766] J. S. Levinson, *Automatic laser calibration, mapping, and localization for autonomous vehicles*. Stanford University, 2011.

[767] R. Mascaro, L. Teixeira, T. Hinzmann, R. Siegwart, and M. Chli, “GOMSF: Graph-Optimization based Multi-Sensor Fusion for Robust UAV Pose Estimation,” in *ICRA*, pp. 1421–1428, IEEE, 2018.

[768] P. Geneva, K. Eckenhoff, and G. Huang, “Asynchronous Multi-Sensor Fusion for 3D Mapping and Localization,” in *ICRA*, IEEE, 2018.

[769] B. Grelsson, A. Robinson, M. Felsberg, and F. S. Khan, “GPS-level accurate camera localization with HorizonNet,” *Journal of Field Robotics*, vol. 37, pp. 951–971, 9 2020.

[770] S. Zhao, Y. Chen, H. Zhang, and J. A. Farrell, “Differential gps aided inertial navigation: A contemplative realtime approach,” *IFAC Proceedings Volumes*, vol. 47, no. 3, pp. 8959–8964, 2014.

[771] F. Zhang, Z. Wang, Y. Zhong, and L. Chen, “Localization Error Modeling for Autonomous Driving in GPS Denied Environment,” *Electronics (Switzerland)*, vol. 11, 2 2022.

[772] H. Shen, Q. Zong, B. Tian, and H. Lu, “Voxel-based localization and mapping for multirobot system in gps-denied environments,” *IEEE Transactions on Industrial Electronics*, vol. 69, pp. 10333–10342, 10 2022.

[773] X. Shan, A. Cabani, and H. Chafouk, “Cooperative localization based on gps correction and ekf in urban environment,” Institute of Electrical and Electronics Engineers Inc., 2022.

[774] A. Couturier and M. A. Akhloufi, “Convolutional neural networks and particle filter for UAV localization,” *https://doi.org/10.1117/12.2585986*, vol. 11758, pp. 108–120, 4 2021.

[775] K. Kim, J. Im, and G. Jee, “Tunnel facility based vehicle localization in highway tunnel using 3d lidar,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, pp. 17575–17583, 10 2022.

[776] C. Xia, Y. Shen, Y. Yang, X. Deng, S. Chen, J. Xin, and N. Zheng, “Onboard sensors-based self-localization for autonomous vehicle with hierarchical map,” *IEEE Transactions on Cybernetics*, 2022.

[777] K. Viana, A. Zubizarreta, and M. Diez, “Robust localization for autonomous vehicles in dense urban areas,” pp. 107–112, Institute of Electrical and Electronics Engineers Inc., 2021.

[778] M. Bürki, L. Schaupp, M. Dymczyk, R. Dubé, C. Cadena, R. Siegwart, and J. Nieto, “Vizard: Reliable visual localization for autonomous vehicles in urban outdoor environments,” in *2019 IEEE Intelligent Vehicles Symposium (IV)*, pp. 1124–1130, IEEE, 2019.

[779] B. Cao, C.-N. Ritter, D. Göhring, and R. Rojas, “Accurate localization of autonomous vehicles based on pattern matching and graph-based optimization in urban environments,” in *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*, pp. 1–6, IEEE, 2020.

[780] N. Carson, S. M. Martin, J. Starling, and D. M. Bevly, “GPS spoofing detection and mitigation using Cooperative Adaptive Cruise Control system,” pp. 1091–1096, Institute of Electrical and Electronics Engineers Inc., 2016.

[781] J. Hardy, J. Strader, J. N. Gross, Y. Gu, M. Keck, J. Douglas, and C. N. Taylor, “Unmanned aerial vehicle relative navigation in GPS denied environments,” pp. 344–352, Institute of Electrical and Electronics Engineers Inc., 2016.

[782] Q. Liu, Y. Mo, X. Mo, C. Lv, E. Mihankhah, and D. Wang, “Secure Pose Estimation for Autonomous Vehicles under Cyber Attacks,” in *IEEE Intelligent Vehicles Symposium (IV)*, 2019.

[783] M. Ángel de Miguel, F. García, and J. M. Armingol, “Improved LiDAR probabilistic localization for autonomous vehicles using GNSS,” *Sensors (Switzerland)*, vol. 20, 6 2020.

[784] S. Yousuf and M. B. Kadri, “Information Fusion of GPS, INS and Odometer Sensors for Improving Localization Accuracy of Mobile Robots in Indoor and Outdoor Applications,” *Robotica*, vol. 39, pp. 250–276, 2 2021.

[785] S. Zahedian, K. F. Sadabadi, and A. Nohekhan, “Localization of autonomous vehicles: proof of concept for a computer vision approach,” *arXiv preprint arXiv:2104.02785*, 2021.

[786] Y. Ding and Z. Fu, “Multi-UAV Cooperative GPS Spoofing Based on YOLO Nano,” *Journal of Cyber Security*, vol. 3, pp. 69–78, 2021.

[787] D. Zhang, C. Lv, T. Yang, and P. Hang, “Cyber-attack detection for autonomous driving using vehicle dynamic state estimation,” *Automotive Innovation*, vol. 4, pp. 262–273, 2021.

[788] Y. Wang, Q. Liu, E. Mihankhah, C. Lv, and D. Wang, “Detection and isolation of sensor attacks for autonomous vehicles: Framework, algorithms, and validation,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 8247–8259, 2021.

[789] W. Afifi, H. A. Hefny, and N. R. Darwish, “Adaptive Kalman Filter for Free GPS Localization with Fuzzy Intersection Method,” *International Journal of Intelligent Engineering and Systems*, vol. 15, pp. 394–405, 2022.

[790] I. Torroba, C. I. Sprague, and J. Folkesson, “Fully-probabilistic terrain modelling and localization with stochastic variational gaussian process maps,” *IEEE Robotics and Automation Letters*, vol. 7, pp. 8729–8736, 10 2022.

[791] W. Liang, K. Li, and Q. Li, “Anti-spoofing Kalman filter for GPS/rotational INS integration,” *Measurement: Journal of the International Measurement Confederation*, vol. 193, 4 2022.

[792] M. Dares, K. W. Goh, Y. S. Koh, C. F. Yeong, E. L. Su, and P. H. Tan, “Automated guided vehicle robot localization with sensor fusion,” in *Computational Intelligence in Machine Learning: Select Proceedings of ICCIML 2021*, pp. 135–143, Springer, 2022.

[793] C. Kwon, W. Liu, and I. Hwang, “Analysis and design of stealthy cyber attacks on unmanned aerial systems,” *Journal of Aerospace Information Systems*, vol. 11, pp. 525–539, 8 2014.

[794] K. Manandhar, X. Cao, F. Hu, and Y. Liu, “Detection of faults and attacks including false data injection attack in smart grid using kalman filter,” *IEEE transactions on control of network systems*, vol. 1, no. 4, pp. 370–379, 2014.

[795] C. Pei, Y. Xiao, W. Liang, and X. Han, “A deviation-based detection method against false data injection attacks in smart grid,” *IEEE access*, vol. 9, pp. 15499–15509, 2021.

[796] Q. Jin, X. Chen, P. Zhang, J. Yuan, and S. Li, “State estimation of wireless sensor networks under false data injection,” in *Journal of Physics: Conference Series*, vol. 2216, p. 012016, IOP Publishing, 2022.

[797] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, “False data injection attacks against state estimation in wireless sensor networks,” pp. 5967–5972, Institute of Electrical and Electronics Engineers Inc., 2010.

[798] Y. Li, H. Lin, and J. Lam, “Optimal filter design for cyber-physical systems under stealthy hybrid attacks,” *International Journal of Robust and Nonlinear Control*, vol. 31, no. 4, pp. 1340–1357, 2021.

[799] Z. Haider and S. Khalid, “Survey on effective gps spoofing countermeasures,” in *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, pp. 573–577, 2016.

[800] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O’Hanlon, and P. M. Kintner, “Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer,” in *Radionavigation Laboratory Conference Proceedings*, 2008.

[801] C. Kwon, W. Liu, and I. Hwang, “Security analysis for Cyber-Physical Systems against stealthy deception attacks,” *Proceedings of the American Control Conference*, pp. 3344–3349, 2013.

[802] J. Su, J. He, P. Cheng, and J. Chen, “A Stealthy GPS Spoofing Strategy for Manipulating the Trajectory of an Unmanned Aerial Vehicle,” in *IFAC-PapersOnLine*, vol. 49, pp. 291–296, Elsevier B.V., 2016.

[803] K. Miao, W.-A. Zhang, and X. Qiu, “An adaptive unscented kalman filter approach to secure state estimation for wireless sensor networks,” *Asian Journal of Control*, vol. 25, no. 1, pp. 629–636, 2023.

[804] J. Lu, W. Wang, L. Li, and Y. Guo, “Unscented Kalman filtering for nonlinear systems with sensor saturation and randomly occurring false data injection attacks,” *Asian Journal of Control*, vol. 23, no. 2, pp. 871–881, 2021.

[805] S. Z. Khan, M. Mohsin, and W. Iqbal, “On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions,” *PeerJ Computer Science*, vol. 7, p. e507, 2021.

[806] J. Bhatti and T. E. Humphreys, “Hostile Control of Ships via False GPS Signals: Demonstration and Detection,” *Navigation*, vol. 64, pp. 51–66, 3 2017.

[807] B. Chen, D. W. Ho, G. Hu, and L. Yu, “Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks,” *IEEE transactions on cybernetics*, vol. 48, no. 6, pp. 1862–1876, 2017.

[808] G. Panice, S. Luongo, G. Gigante, D. Pascarella, C. Di Benedetto, A. Vozella, and A. Pescapè, “A svm-based detection approach for gps spoofing attacks to uav,” in *2017 23rd International Conference on Automation and Computing (ICAC)*, pp. 1–11, IEEE, 2017.

[809] X. Wei and B. Sikdar, “Impact of GPS time spoofing attacks on cyber physical systems,” in *2019 IEEE international conference on industrial technology (ICIT)*, pp. 1155–1160, IEEE, 2019.

[810] H. Sathaye, M. Strohmeier, V. Lenders, and A. Ranganathan, “An experimental study of {GPS} spoofing and takeover attacks on {UAVs},” in *31st USENIX Security Symposium (USENIX Security 22)*, pp. 3503–3520, 2022.

[811] K. C. Zeng, S. Liu, Y. Shu, D. Wang, H. Li, Y. Dou, G. Wang, and Y. Yang, "All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems," in *Usenix Security Symposium*, 2018.

[812] D. Mendes, N. Ivaki, and H. Madeira, "Effects of GPS spoofing on unmanned aerial vehicles," in *2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC)*, pp. 155–160, IEEE, 2018.

[813] O. Thapliyal and I. Hwang, "Data-driven Cyberattack Synthesis against Network Control Systems," 11 2022.

[814] J. Guo, L. Li, J. Wang, and K. Li, "Cyber-Physical System-Based Path Tracking Control of Autonomous Vehicles under Cyber-Attacks," *IEEE Transactions on Industrial Informatics*, 2022.

[815] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg, and R. Candell, "A Survey of Physics-based Attack Detection in Cyber-Physical Systems," *ACM Computing Surveys (CSUR)*, vol. 51, no. 4, pp. 1–36, 2018.

[816] M. Schreiber, H. Königshof, A.-M. Hellmund, and C. Stiller, "Vehicle Localization with Tightly Coupled GNSS and Visual Odometry," in *2016 IEEE Intelligent Vehicles Symposium (IV)*, IEEE, 2016.

[817] B.-H. Lee, J.-H. Song, J.-H. Im, S.-H. Im, M.-B. Heo, and G.-I. Jee, "GPS/DR Error Estimation for Autonomous Vehicle Localization," *Sensors*, vol. 15, no. 8, pp. 20779–20798, 2015.

[818] R. Piché, "Online Tests of Kalman Filter Consistency," *International Journal of Adaptive Control and Signal Processing*, vol. 30, no. 1, pp. 115–124, 2016.

[819] I. V. Nikiforov, "A generalized change detection problem," *IEEE Transactions on Information theory*, vol. 41, no. 1, pp. 171–187, 1995.

[820] J. J. Gertler, "Survey of Model-Based Failure Detection and Isolation in Complex Plants," *IEEE Control Systems Magazine*, vol. 8, no. 6, pp. 3–11, 1988.

[821] D. P. Malladi and J. L. Speyer, "A generalized shiryayev sequential probability ratio test for change detection and isolation," *IEEE Transactions on Automatic Control*, vol. 44, no. 8, pp. 1522–1534, 1999.

[822] D. Dionne, H. Michalska, Y. Oshman, and J. Shinar, "Novel adaptive generalized likelihood ratio detector with application to maneuvering target tracking," *Journal of guidance, control, and dynamics*, vol. 29, no. 2, pp. 465–474, 2006.

[823] A. S. Willsky, "A survey of design methods for failure detection in dynamic systems," *Automatica*, vol. 12, no. 6, pp. 601–611, 1976.

[824] S. Dasgupta, M. Rahman, M. Islam, and M. Chowdhury, "A Sensor Fusion-Based GNSS Spoofing Attack Detection Framework for Autonomous Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, pp. 23559–23572, 12 2022.

[825] R. V. Beard, *Failure accommodation in linear systems through self-reorganization.* PhD thesis, Massachusetts Institute of Technology, 1971.

[826] H. L. Jones, *Failure detection in linear systems.* PhD thesis, Massachusetts Institute of Technology, 1973.

[827] P. F. Roysdon and J. A. Farrell, "Gps-ins outlier detection & elimination using a sliding window filter," in *2017 American Control Conference (ACC)*, pp. 1244–1249, 2017.

[828] J. Guo, L. Li, J. Wang, and K. Li, "Cyber-physical system-based path tracking control of autonomous vehicles under cyber-attacks," *IEEE Transactions on Industrial Informatics*, 2022.

[829] N. Sadeghzadeh-Nokhodberiz, N. Meskin, and S. Hasanzadeh, "Modified Particle Filters for Detection of False Data Injection Attacks and State Estimation in Networked Nonlinear Systems," *IEEE Access*, vol. 10, pp. 32728–32741, 2022.

[830] M. Khalaf, A. Youssef, and E. El-Saadany, “A particle filter-based approach for the detection of false data injection attacks on automatic generation control systems,” in *2018 IEEE Electrical Power and Energy Conference (EPEC)*, pp. 1–6, IEEE, 2018.

[831] A. Neish, S. Lo, Y. H. Chen, and P. Enge, “Uncoupled Accelerometer Based GNSS Spoof Detection for Automobiles Using Statistic and Wavelet Based Tests,” *Proceedings of the 31st International Technical Meeting of the Satellite Division of the Institute of Navigation, ION GNSS+ 2018*, pp. 2938–2962, 9 2018.

[832] D. Marnach, S. Mauw, M. Martins, and C. Harpes, “Detecting meaconing attacks by analysing the clock bias of gnss receivers,” *Artificial Satellites*, vol. 48, no. 2, pp. 63–83, 2013.

[833] A. Valdes and K. Skinner, “Probabilistic alert correlation,” in *Recent Advances in Intrusion Detection: 4th International Symposium, RAID 2001 Davis, CA, USA, October 10–12, 2001 Proceedings 4*, pp. 54–68, Springer, 2001.

[834] J. Levinson, J. Askeland, J. Becker, J. Dolson, D. Held, S. Kammel, J. Z. Kolter, D. Langer, O. Pink, V. Pratt, *et al.*, “Towards fully autonomous driving: Systems and algorithms,” in *Intelligent Vehicles Symposium (IV), 2011 IEEE*, pp. 163–168, IEEE, 2011.

[835] X. Wang, C. Toth, D. Grejner-Brzezinska, and A. Masiero, “Collaborative Navigation: Supporting PNT System Operational Anomaly Detection,” *10th IFAC International Symposium on Advances in Automotive Control*, 2022.

[836] S. Vasudevan, “Data fusion with gaussian processes,” *Robotics and Autonomous Systems*, vol. 60, no. 12, pp. 1528–1544, 2012.

[837] Z. Wang and F. Xiao, “An improved multisensor data fusion method and its application in fault diagnosis,” *IEEE Access*, vol. 7, pp. 3928–3937, 2018.

[838] International Organization for Standardization, *ISO 26262: Road Vehicles - Functional Safety*, 2011.

[839] International Organization for Standardization, *ISO/PAS 21448: Road Vehicles - Safety of the Intended Function*, 2019.

[840] Underwriter Laboratories Tech Panel, *UL4600: Standard for Evaluation of Autonomous Products*, 2020.

[841] N. G. Leveson and J. P. Thomas, *STPA handbook*, vol. 3. MIT Press, 2018.

[842] C. Becker, J. C. Brewer, L. Yount, *et al.*, “Safety of the intended functionality of lane-centering and lane-changing maneuvers of a generic level 3 highway chauffeur system,” tech. rep., United States. National Highway Traffic Safety Administration. Electronic, 2020.

[843] D. Heß, J. Oehlerking, M. Woehrle, and J. Sanchez Cubillo, “The UnCoVerCPS Verification Approach to Automated Driving,” in *20th International Forum on Advanced Microsystems for Automotive Applications, AMAA 2016*, 2016.

[844] H. S. Mahajan, T. Bradley, and S. Pasricha, “Application of systems theoretic process analysis to a lane keeping assist system,” *Reliability Engineering & System Safety*, vol. 167, pp. 177–183, 2017.

[845] G. C. Kölln, M. Klicker, and S. Schmidt, “Comparison of hazard analysis methods with regard to the series development of autonomous vehicles,” in *2019 IEEE Intelligent Transportation Systems Conference (ITSC)*, pp. 2969–2975, 2019.

[846] J. Brewer, C. Becker, J. Pollard, L. Yount, *et al.*, “Functional safety assessment of a generic automated lane centering system and related foundational vehicle systems,” tech. rep., United States. Department of Transportation. National Highway Traffic Safety, 2018.

[847] G. Koelln, M. Klicker, and S. Schmidt, “Comparison of the Results of the System Theoretic Process Analysis for a Vehicle SAE Level four and five,” in *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*, pp. 1–6, 2020.

[848] A. Abdulkhaleq, M. Baumeister, H. Böhmert, and S. Wagner, "Missing no Interaction—Using STPA for Identifying Hazardous Interactions of Automated Driving Systems," *International Journal of Safety Science*, vol. 2, no. 01, pp. 115–24, 2018.

[849] G. Macher, H. Sporer, R. Berlach, E. Armengaud, and C. Kreiner, "SAHARA: a security-aware hazard and risk analysis method," in *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 621–624, IEEE, 2015.

[850] S. M. Sulaman, A. Beer, M. Felderer, and M. Höst, "Comparison of the FMEA and STPA safety analysis methods–a case study," *Software quality journal*, vol. 27, no. 1, pp. 349–387, 2019.

[851] L. Capito and K. A. Redmill, "Methodology for hazard identification and mitigation strategies applied to an overtaking assistant adas," in *2021 IEEE International Intelligent Transportation Systems Conference (ITSC)*, pp. 3972–3977, 2021.

[852] S. Khastgir, S. Brewerton, J. Thomas, and P. Jennings, "Systems approach to creating test scenarios for automated driving systems," *Reliability engineering & system safety*, vol. 215, p. 107610, 2021.

[853] L. Capito, K. Redmill, and U. Ozguner, "Model-based decomposition and backtracking framework for probabilistic risk assessment in automated vehicle systems," in *2021 International Topical Meeting on Probabilistic Safety Assessment and Analysis, PSA 2021*, American Nuclear Society, 2021.

[854] Z. He, L. Capito, K. Redmill, F. Özgüner, and Ü. Özgüner, "Risk analysis for vehicle–pedestrian interaction with extended sensing," *Towards Human-Vehicle Harmonization*, vol. 3, p. 65, 2023.

[855] A. C. Bukhari, I. Tusseyeva, Y.-G. Kim, *et al.*, "An intelligent real-time multi-vessel collision risk assessment system from vts view point based on fuzzy inference system," *Expert systems with applications*, vol. 40, no. 4, pp. 1220–1230, 2013.

[856] M. Althoff and A. Mergel, "Comparison of markov chain abstraction and monte carlo simulation for the safety assessment of autonomous cars," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 4, pp. 1237–1247, 2011.

[857] L. Capito and K. Redmill, "Methodology for Hazard Identification and Mitigation Strategies Applied to an Overtaking Assistant ADAS," in *2021 IEEE International Intelligent Transportation Systems Conference (ITSC)*, pp. 3972–3977, 2021.

[858] F. Warg, M. Gassilewski, J. Tryggvesson, V. Izosimov, A. Werneman, and R. Johansson, "Defining autonomous functions using iterative hazard analysis and requirements refinement," in *International Conference on Computer Safety, Reliability, and Security*, pp. 286–297, Springer, 2016.

[859] T. Stolte, G. Bagschik, A. Reschka, and M. Maurer, "Hazard analysis and risk assessment for an automated unmanned protective vehicle," in *2017 IEEE Intelligent Vehicles Symposium (IV)*, pp. 1848–1855, IEEE, 2017.

[860] G. Bagschik, A. Reschka, T. Stolte, and M. Maurer, "Identification of potential hazardous events for an unmanned protective vehicle," in *2016 IEEE Intelligent Vehicles Symposium (IV)*, pp. 691–697, IEEE, 2016.

[861] A. Wardziński, "Safety assurance strategies for autonomous vehicles," in *International Conference on Computer Safety, Reliability, and Security*, pp. 277–290, Springer, 2008.

[862] S. Khastgir, H. Sivencrona, G. Dhadyalla, P. Billing, S. Birrell, and P. Jennings, "Introducing asil inspired dynamic tactical safety decision framework for automated vehicles," in *2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC)*, pp. 1–6, IEEE, 2017.

[863] F. Warg, M. Skoglund, A. Thorsén, R. Johansson, M. Brännström, M. Gyllenhammar, and M. Sanfridson, "The quantitative risk norm-a proposed tailoring of hara for ads," in *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, pp. 86–93, IEEE, 2020.

[864] S. Puch, M. Fränzle, and S. Gerwinn, "Quantitative risk assessment of safety-critical systems via guided simulation for rare events," in *International Symposium on Leveraging Applications of Formal Methods*, pp. 305–321, Springer, 2018.