CARMEN+ UTC:
Center for Automated Vehicle Research with Multimodal AssurEd Navigation

Highly Automated Transportation Systems Research
University Transportation Centers Program

FY2023 Semi-Annual Progress Report
(Covering: October 1, 2023 – March 31, 2024)
Submission: April 30, 2024

P.I.:
Zak M. Kassas, Ph.D.
Director, US DOT Center for Automated Vehicles Research with Multimodal AssurEd Navigation (CARMEN+)
Professor, Electrical & Computer Engineering
The Ohio State University
Phone: 614-247-6306
Email: kassas.2@osu.edu

Project Info:
Grant No. 69A3552348327
DUNS: 832127323
EIN #: 31-6025986
Office of Sponsored Projects
1960 Kenny Rd.
Columbus, OH 43210-1016
Project Effective: June 1, 2023
Project End: May 31, 2029

Consortium Members

NOTICE OF RESTRICTION ON DISCLOSURE AND USE OF DATA
Pages [all pages] of this document may contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure. Such information shall be used or disclosed only for evaluation purposes or in accordance with a financial assistance or loan agreement between the submitter and the Government. The Government may use or disclose any information that is not appropriately marked or otherwise restricted, regardless of source.

May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.
**Section 1: Accomplishments**

*What are the major goals of the program?*

- Thrust 1: Identify Existing and Emerging Cybersecurity Threats to HATS
- Thrust 2: Analyze Threat Scenarios and Cybersecurity Risks to HATS
- Thrust 3: Develop Cyber-resilient Mitigation Methods
- Thrust 4: Testing and Validation in Real-world Jammed, Spoofed, and Cyber Compromised Environments

*What was accomplished under these goals?*

**Data-driven Modeling and Anomaly Detection of Attacked HATS**

- Data Preprocessing and Feature Engineering: We utilized the Honda Driving dataset (HDD) and conducted extensive preprocessing and feature engineering to capture vehicle movement dynamics and GPS signal characteristics.

- Machine Learning Algorithms and Data Fusion Techniques:
  - We have developed machine learning algorithms specifically designed to analyze discrepancies and anomalies within GPS data streams. Leveraging data from in-vehicle sensors such as the Gyroscope, Speedometer, and Steering Angle sensors, our algorithms predict the expected displacement of the vehicle. This predicted displacement is continuously compared with the GPS-provided displacement to detect and identify potential spoofing attacks accurately. Also, GPS and speedometer provided speed are continuously compared to enhance the detection accuracy.
  - Integration of data from multiple sensors, including GPS, Inertial Measurement Unit (IMU), and vehicle Controller Area Network (CAN) bus data, was explored to enhance detection accuracy and robustness. Our algorithms utilize this integrated sensor data to improve the reliability of spoofing attack detection, particularly focusing on identifying turn-by-turn attacks, overshoot attacks, and stop attacks. By continuously monitoring and analyzing the discrepancies between predicted and GPS-provided displacements, our system can promptly identify deviations that are indicative of spoofing attempts.
  - The integration of machine learning techniques with real-time sensor data analysis enables proactive detection and response to potential spoofing threats, thereby ensuring the integrity and trustworthiness of GPS-based navigation systems in highly automated vehicles. This approach contributes significantly to the overall security and reliability of GPS-based navigation systems, enhancing the safety and performance of autonomous driving technologies.

**Fuzzing Autonomous Vehicles via Traffic-Rule Guided Symbolic Execution;**

- Lin and his collaborators recently discovered an important attack that uncover vulnerabilities at the intersection of wearable devices and automated control systems, with a particular emphasis on the use of smart glasses as an access point to infiltrate security-critical automated control chains without user verification or interaction. Their study underscores the substantial risks associated particularly with transportation systems, notably Tesla vehicles, when security measures predominantly rely on the entry point's security and minimal user verification, assuming full trust in prior nodes within automated control chains.

*May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.*
The practical implications of these vulnerabilities were rigorously tested on Tesla vehicles, which are managed through software and automation tools such as Apple Shortcuts or IFTTT. The findings vividly demonstrate how innovative, non-invasive attacks—such as those based on contactless methods, speaker independence, and electromagnetic interference—can successfully manipulate critical functionalities. Specifically, these attacks were shown to unlock doors and initiate the remote start of Tesla vehicles, all performed without any physical interaction and while the victim's smartphone remained in a lock-screen state.

These significant results highlight an urgent need for advancing security measures within the transportation sector, particularly in the integration of wearable technologies with automotive control systems. The study stresses the importance of implementing more robust security frameworks to prevent unauthorized control over connected, automated vehicles, showcasing a critical area for future research and development in automotive cybersecurity.

The Future of HD Mapping: Crowdsourcing to Improve PNT Resilience and Safety

- We have performed literature review on how HD Maps are created, including online and offline approaches. Next the structure of HD Maps was analyzed; note that currently there is no standard structure or format, making it difficult to aggregate different types of HD Maps. The most common part of HD Maps are the first three layers that contain information about (1) the road geometry and topology, (2) lane types, pavement markings, boundaries, etc., and (3) roadside furniture such as, traffic signals, stop signs, buildings along the corridor. Additional layers typically include time-dependent information such as road closures, congestion, etc.

- We have carried out a performance comparison of HD Map creation methods and available datasets with a focus on the on-the-fly solutions. Note that most of the techniques are based on using neural network and deep learning. In addition, we have reviewed suitable HD Map change detection architectures that are of great importance to achieve a live HD Map system in the future. We have implemented a basic model to experience with visual sensor data, using the most popular Bird’s Eye View (BEV) technique. Latent Diffusion Model and Transformers were tested for accuracy and execution speed.

- In our studies, four datasets created to support autonomous driving research have been considered, including Argoverse2, nuScenes, Waymo, and KITTI. Except for KITTI, these datasets were produced in recent years using state-of-the-art sensor technologies and included large number of scenes in various weather conditions. For HD Map generation, four methods have been investigated, including HDMapNet, VectorMapNet, MapTR, and PivotNet, in the order of their introduction. We performed performance evaluation using the mean average precision (mAP) metrics for extracting road boundary, lane separator and pedestrian crossing features. The performance was analyzed with respect to the two most recent test datasets, nuScenes and Argoverse2, and showed comparable results.

P1. LiDAR Spoofing Meets the New-Gen: Capability Improvements, Broken Assumptions, and New Attack Strategies

LiDAR is an indispensable sensor for precise long- and wide-range 3D sensing, which directly benefited the recent rapid deployment of autonomous driving (AD). Meanwhile, such a safety-critical application strongly motivates its security research. A recent line of research finds that one can manipulate the LiDAR point cloud and fool object detectors by firing malicious lasers against LiDAR. However, these efforts face
3 critical research gaps: (1) considering only one specific LiDAR (VLP-16); (2) assuming unvalidated attack capabilities; and (3) evaluating object detectors with limited spoofing capability modeling and setup diversity. To fill these critical research gaps, we conduct the first large-scale measurement study on LiDAR spoofing attack capabilities on object detectors with 9 popular LiDARs, covering both first- and new-generation LiDARs, and 3 major types of object detectors trained on 5 different datasets. To facilitate the measurements, we (1) identify spoofer improvements that significantly improve the latest spoofing capability, (2) identify a new object removal attack that overcomes the applicability limitation of the latest method to new-generation LiDARs, and (3) perform novel mathematical modeling for both object injection and removal attacks based on our measurement results. Through this study, we are able to uncover a total of 15 novel findings, including not only completely new ones due to the measurement angle novelty, but also many that can directly challenge the latest understandings in this problem space. We also discuss defenses.

P2. Invisible Reflections: Leveraging Infrared Laser Reflections to Target Traffic Sign Perception

All vehicles must follow the rules that govern traffic behavior, regardless of whether the vehicles are human-driven or Connected Autonomous Vehicles (CAVs). Road signs indicate locally active rules, such as speed limits and requirements to yield or stop. Recent research has demonstrated attacks, such as adding stickers or projected colored patches to signs, that cause CAV misinterpretation, resulting in potential safety issues. Humans can see and potentially defend against these attacks. But humans cannot detect what they cannot observe. We have developed an effective physical-world attack that leverages the sensitivity of filterless image sensors and the properties of Infrared Laser Reflections (ILRs), which are invisible to humans. The attack is designed to affect CAV cameras and perception, undermining traffic sign recognition by inducing misclassification. In this work, we formulate the threat model and requirements for an ILR-based traffic sign perception attack to succeed. We evaluate the effectiveness of the ILR attack with real-world experiments against two major traffic sign recognition architectures on four IR-sensitive cameras. Our black-box optimization methodology allows the attack to achieve up to a 100% attack success rate in indoor, static scenarios and a ≥80.5% attack success rate in our outdoor, moving vehicle scenarios. We find the latest state-of-the-art certifiable defense is ineffective against ILR attacks as it mis-certifies ≥33.5% of cases. To address this, we propose a detection strategy based on the physical properties of IR laser reflections which can detect 96% of ILR attacks.

P3. Understanding the Internet-Wide Vulnerability Landscape for ROS-based Robotic Vehicles

Due to the cyber-physical nature of robotic vehicles, security is especially crucial, as a compromised system not only exposes privacy and information leakage risks, but also increases the risk of harm in the physical world. As such, in this paper, we explore the current vulnerability landscape of robotic vehicles exposed to and thus remotely accessible by any party on the public Internet. Focusing particularly on instances of the Robot Operating System (ROS), a commonly used open-source robotic software framework, we performed new Internet-wide scans of the entire IPv4 address space, identifying, categorizing, and analyzing the ROS-based systems we discovered. We further performed the first measurement of ROS scanners in the wild by setting up ROS honeypots, logging traffic, and analyzing the traffic we received. We found over 190 ROS systems on average being regularly exposed to the public Internet and discovered new trends in the exposure of different types of robotic vehicles, suggesting increasing concern regarding the cybersecurity of today’s ROS-based robotic vehicle systems.
P4. A Cross-Verification Approach with Publicly Available Map for Detecting Off-Road Attacks against Lane Detection Systems

Automated Lane Centering (ALC) is one of the most popular autonomous driving (AD) technologies available in many commodity vehicles. ALC can reduce the human driver’s efforts by taking over their steering work. However, recent research alerts that ALC can be vulnerable to off-road attacks that lead victim vehicles out of their driving lane. To be secure against off-road attacks, this paper explores the potential defense capability of low-quality localization and publicly available maps against off-road attacks against autonomous driving. We design the first map-fusion-based off-road attack detection approach, LaneGuard, LaneGuard detects off-road attacks based on the difference between the observed road shape and the driver predefined route shape. We evaluate LaneGuard on large-scale real-world driving traces consisting of 80 attack scenarios and 11,558 benign scenarios. We find that LaneGuard can achieve an attack detection rate of 89% with a 12% false positive rate. In real-world highway driving experiments, LaneGuard exhibits no false positives while maintaining a near-zero false negative rate against simulated attacks.

P5. Investigation of LiDAR for Traffic Monitoring with Emphasis on Heavy Duty Trucks

We applied LiDAR technology to the specific task of traffic monitoring focusing on Heavy Duty Trucks, using a side-fire LiDAR configuration setup. We assessed LiDAR’s capability to not only collect basic traffic data, such as vehicle counts and speeds, similar to current systems but also to gather high-resolution data necessary for future transportation needs. This includes precise vehicle positions, dimensions, and detailed movement patterns. Tests conducted in both urban and rural settings showed promising results. In an urban environment, LiDAR’s vehicle counting accuracy ranged from 87% to 110% when compared to traditional sensors, while in rural areas, it successfully recorded detailed vehicle trajectories at a 0.1-second resolution. Additionally, it precisely determined the lateral positions of heavy-duty trucks, important for evaluating autonomous truck safety. The enhanced traffic data obtained can aid in identifying unusual vehicle behaviors, contributing to road safety analyses and emissions modeling.

P6. Integrating Infrastructure-based Sensing with Traffic Control

Professor Jayakrishnan, with graduate student Pengyuan Sun, completed research that leveraged 25 instrumented intersections in the City of Irvine associated with a DOE-sponsored vehicle technology office project. This research implemented an eco-driving algorithm designed for use in human-driven vehicles to mitigate the problems of traffic delay and speed fluctuation at signalized urban intersections. The algorithm leverages upstream traffic flow data obtained from in-road, LiDAR, or connected vehicle information to adjust signal timing and control intersection flow rates. It operates by calculating the arrival time of vehicles based on the current signal plan and intersection speeds obtained through infrastructure-based LiDAR, subsequently issuing two stages of speed advice to one vehicle per signal phase, with other vehicles following standard car-following models. The methodology ensures timely vehicle arrival at intersections as per kinematic wave theory and car-following principles. Even when vehicles ignore the algorithm’s speed recommendations, it adapts seamlessly in the next signal cycle. Tested under various conditions of traffic congestion and signal timing, the algorithm successfully enhances traffic throughput and average speed, and lowers fuel consumption and emissions, demonstrating its effectiveness in promoting eco-driving practices.

Chance-Constrained Collision Avoidance Based Motion Planning within Cooperative Perception

May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.
• Developing and implementing processing pipeline and simulation framework
• Using a late fusion scheme to realize cooperative perception.
• Incorporating uncertainty prediction into our object detection algorithm.
• Merging detection outputs from connected vehicles using predicted uncertainties.
• Evaluating 3D object detection and tracking performance.
• Merging bounding boxes of the same object detected by all connected vehicles using the corresponding predicted uncertainties of each bounding box coordinate, to obtain a more refined bounding box.
• Different bounding box strategies were simulated and compared for both synchronous and asynchronous data transmission settings.
• Our box fusion method outperforms standard Non-Max Suppression-based (NMS) post-processing method.
• We were able to achieve better results than the state-of-the-art for both object detection and tracking on the V2V4Real dataset with our bounding box merging algorithm.

Evaluation of Cybersecurity Risks in Smart City Environments

Over the past six months, we focused on conducting extensive literature reviews to explore various approaches from different perspectives and to identify novel algorithms that could mitigate the impact of cybersecurity threats in smart city environments. This comprehensive review has enhanced our theoretical foundation and identified robust algorithms suitable for application in real-world scenarios. One of the primary achievements of this period was the implementation of a cooperative navigation framework at a smart intersection. We successfully implemented a cooperative collision avoidance algorithm on one ego vehicle, enabling the velocity profile of this vehicle to adapt based on the threat levels posed by other vehicles under various scenarios. This enhancement has effectively optimized vehicle coordination and safety at smart intersections.

Further developing our project, we created a multi-agent system (MAS) consensus control framework. We demonstrated its application in a highway merging scenario, which allowed multiple ego vehicles to maintain consistent speed and distance without collision. The consensus control problem involves the convergence of states of all vehicles to a common value. It implies that each vehicle can access other vehicles’ states, known as the neighboring vehicles, using either a communication network or sensing devices. However, when applying the same MAS framework to other merging scenarios, we observed potential collision risks. This led to an innovative development where we incorporated safety filter within the MAS framework to ensure collision-free operations. This adaptation significantly enhanced the safety and reliability of the system under varied conditions.

Privacy-preserving Machine Learning Models for Traffic Forecasting

• Privacy Preservation: A novel privacy-preserving location reporting scheme was developed based on Inner Product Functional Encryption (IPFE). This scheme effectively safeguards the privacy of driver route information while enabling access to encrypted data necessary for predicting traffic congestion and creating accurate traffic forecast density maps.

• Real-time Traffic Forecasting: A deep learning (DL)-based model was developed, integrating Conv-LSTM and Bi-LSTM modules with a Squeeze-and-Excitation (SE) module. This hybrid

May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.
architecture captures both spatial and temporal traffic patterns, enhancing forecast performance and accuracy. The system demonstrated high prediction accuracy with a mean absolute error of less than 10% for a 60-minute forecasting horizon.

- **Scalability and Efficiency**: The project achieved scalability and efficiency in real-time deployment under dynamic traffic conditions. The system supports an increasing volume of drivers and expanding geographic coverage while maintaining minimal latency, communication and computational overheads.
- **Secure Communication**: The project developed and utilized secure communication protocols and cryptography techniques to ensure the integrity, security, and confidentiality of the data exchanged between system entities.

**Timing-based Attacks and Mitigation for Safe HATS**

Within the Intelligent Transportation Systems, vehicular networks have received much attention in recent work. The vehicle-to-everything (V2X) networks allow information about traffic condition and other information about road conditions to be disseminated, allowing vehicles to take early action to mitigate the effect of such undesired events. As vehicles navigate, they also perform sensing to map out their physical surroundings. Integrated Sensing and Communication (ISAC) can accommodate better communication and sensing rates than time sharing. Within the V2X (and even more so with ISAC) models, the communication is subject to passive eavesdropping from targets or malicious nodes along the travel route, motivating a theoretical analysis of secure communication limits.

Our research considered an information theoretic model of integrated sensing and communication, allowing us to better characterize the theoretical limits of sensing and reliable, secure communication. Our model is a communication scheme where the transmitter tries to reliably communicate with a legitimate receiver, sense a target, and obfuscate as much of the message from the eavesdropper as possible. In the model, the transmitter can take actions to improve sensing and communication performance. The transmitter also observes feedback, which is used improve communication and localize the target or eavesdropper. A possible practical realization of the transmitter actions is the design of beam forming vectors to improve the advantage of the legitimate receiver over the eavesdropper. The feedback can represent observations of reflected waveforms. In another paper, we considered the limits of this model in the presence of low latency constraints. We modified the model by removing the encoders’ dependence on the channel feedback. We also derived an achievable region for fixed finite length communication and specific reliability, security, and sensing thresholds.

**Use of Mega-Constellations such as Starlink as a Backup for traditional GNSS**

Since the CARMEN+ UTC kickoff, we have been studying the possibility of using signals from mega-constellations of LEO satellites designed for broadband communications as a backup to traditional GNSS for PNT. Before the kickoff, we had already identified structures in Starlink signals that will be useful for measuring the time of arrival (TOA) of Starlink frames. But whether such frames could be used to form pseudorange measurements that are useful for PNT remained an open question.

The answer depends on the beam patterns and scheduling, proportion of predictable frame content, and frame timing properties of the Starlink signals. Our findings for this reporting period are as follows:

1. Up to 16 unique Starlink satellites could, in principle, simultaneously illuminate the same service cell – two on each of 8 channels – without violating the FCC bounds on effective power flux density (EPFD). This is an encouraging result as regards exploiting Starlink as a PNT source. In practice,
we have verified illumination by up to three so-called assigned beams using an agile antenna system.

2. We have developed and verified a simple heuristic by which Starlink satellites likely to be directing an assigned beam to a given service cell may be predicted. Our heuristic is 94% effective at finding at least one assigned beam in each fixed assignment interval.

3. We have found numerous serious anomalies in Starlink frame timing. These complicate formation of easily-modeled pseudorange measurements.

**Monitoring GNSS Interference from LEO**

GNSS receivers in Low Earth Orbit (LEO) are a proven asset for detecting, classifying, and geolocating terrestrial GNSS interference that can be a danger to civil aviation, maritime, or ground vehicle traffic. Emitter geolocation from LEO offers worldwide coverage with a frequent refresh rate, making it possible to maintain a common operating picture of terrestrial sources of interference. We have developed and experimentally verified several techniques for LEO-based interference monitoring. Our key findings:

1. Since August 2023 there has been an alarming rise of GNSS spoofing across the Middle East and Eastern Europe. For the first time, GNSS spoofing has significantly affected commercial aviation.
2. It is possible to locate sources of GNSS spoofing to within 500 meters using pseudorange and Doppler measurements from LEO GNSS receivers provided that the spoofed navigation data are also extractable.
3. It is possible to locate sources of GNSS spoofing to within 3km with only a single spoofed channel’s Doppler time history.

**Joint Design of Signals for Communication and Ranging**

Today’s wireless communication networks are experiencing an ever-growing demand not only for traditional communications but also for positioning, navigation, and timing services, especially accurate user localization. We developed techniques to guide optimal design of waveforms to simultaneously satisfy range precision and communications throughput requirements.

**Enhanced Cybersecurity via Smart Antenna Technology for V2X**

- During the past six months, our team has analyzed several possible CV2X/V2X antenna design candidates via full-wave electromagnetic numerical model simulations. Out of these design candidates, we have down selected and optimized one of the best design whose simulated performance met desired pattern and gain properties suitable for beamforming operations. Our next step is to fabricate and test a prototype antenna to validate simulated performance.
- The specific technical objective of the Year-1 research effort aims to develop a compact inexpensive V2X/C-V2X antenna system design which has 4 antenna elements with suitable gain and pattern characteristics for achieving optimal beamforming and interference-nulling operations. This approach is superior to conventional multiple in multiple out (MIMO) approaches and can achieve superior signal-to-interference-and-noise ratio improvement at the RF front end when used with appropriate electronics.
- We developed an optimized 4-element C-V2X/V2X antenna design via full-wave electromagnetic numerical model simulations. The design is compact and has a diameter of 9.2 cm and height of
2.3 cm. The antenna performance of this design was optimized for supporting MIMO and beamforming operations for enhanced communication security and robustness.

**Using Infrastructure to Boost Safety in a PNT World**

During this reporting period, Dr. Chandra Bhat’s research team at UT Austin have planned and successfully implemented an experimental test bed for recording and categorizing pedestrian-vehicle interactions around intersection crosswalks and right-turn yielding areas. This allows for the study of the role of infrastructure in facilitating an improved robustness in PNT, and also helps to identify specific interactions that a future PNT system may improve.

**Performance analysis of opportunistic ARAIM for navigation with GNSS signals fused with terrestrial signals of opportunity**

Integrity monitoring of a vehicular navigation system that utilizes multi-constellation global navigation satellite systems (GNSS) signals fused with terrestrial signals of opportunity (SOPs) was considered. An opportunistic advanced receiver autonomous integrity monitoring (OARAIM) framework is developed to detect faults and calculate protection levels (PLs). The influence of fusing SOPs on the integrity performance is analyzed. It is shown that fusing a single SOP with GNSS signals essentially increases both the horizontal PL (HPL) and vertical PL (VPL), while fusing two or more SOPs could reduce the PLs and improves fault detection. Performance sensitivity analysis for the probability of SOP fault and user range error is conducted to characterize the fault-free HPL under different regimes. Experimental results on an unmanned aerial vehicle (UAV) navigating with GPS signals fused with cellular SOPs are presented to validate the effectiveness of the OARAIM framework and demonstrate the analysis of the integrity performance in the horizontal direction.

**No GPS no problem: exploiting cellular OFDM-based signals for accurate navigation**

This project developed a receiver that could exploit downlink orthogonal frequency-division multiplexing (OFDM)-based cellular signals to navigate opportunistically to meter-level accuracy in a real-world GPS-denied environment. The proposed receiver exploits signals from multiple logical antenna ports simultaneously, which dramatically improves the receiver’s sensitivity. The efficacy of the proposed receiver is demonstrated experimentally in an environment under intentional GPS jamming, in which the ground vehicle-mounted receiver navigated for 5 km in 180 s. The receiver was able to acquire and track signals from seven long-term evolution (LTE) eNodeBs, one of which was more than 25 km away, achieving a 2-D position root mean-squared error (RMSE) of 2.6 m.

**Unveiling Starlink LEO satellite OFDM-like signal structure enabling precise positioning**

This project unveiled the unknown structure of Starlink low Earth orbit (LEO) satellites’ orthogonal frequency division multiplexing (OFDM)-like reference signals (RSs). The spectrum of Starlink’s downlink signals is presented, and the frame length is estimated. A blind receiver is proposed, which acquires via a sequential generalized likelihood ratio test multiple satellites, estimates their RSs and respective Doppler, and tracks their carrier and code phases. Experimental results are presented showing six tracked Starlink LEO satellites, three of which transmitted pure tones, whereas the other transmitted OFDM-like signals. The achieved horizontal positioning error with the six satellites was 6.5 m.
Ephemeris tracking and error propagation analysis of LEO satellites with application to opportunistic navigation

A comprehensive study was performed for low Earth orbit (LEO) space vehicles (SVs) tracking by a receiver opportunistically extracting navigation observables from their downlink radio frequency signals. First, a framework to characterize the LEO SVs orbital motion process noise covariance is developed. Second, the tracking performance via an extended Kalman filter (EKF) is analyzed via comprehensive Monte Carlo simulations for three different sets of observables: 1) pseudorange, 2) Doppler, and 3) fused pseudorange and Doppler measurements. Third, experimental results are presented demonstrating the efficacy of the opportunistic tracking framework in refining the ephemeris of a LEO SV from two-line element (TLE) files. Fourth, the error propagation from the LEO SVs state space to the measurement space and from the measurement space to the receiver’s state space is analyzed in the context of stationary receiver localization. Bounds on the magnitude of pseudorange and Doppler residuals are first derived, and the magnitude of the receiver’s estimation error is then characterized as a function of errors in the LEO SVs state space. Fifth, experimental results are presented of a stationary receiver tracking an Orbcomm LEO SV by fusing carrier phase observables via an EKF. The tracked LEO ephemeris is then used to localize another stationary receiver, showing a reduction in the receiver’s initial horizontal error from 13,476 m to 343 m after just over 6 min. In contrast, it is shown that if the SGP4-propagated ephemeris was used in the EKF to localize the receiver, the error is reduced to 6,852 m, but the filter becomes inconsistent.

Joint Doppler and azimuth DOA tracking for positioning with Iridium LEO satellites

A receiver capable of estimating the Doppler and azimuth direction-of-arrival (DOA) of Iridium NEXT low Earth orbit (LEO) signals of opportunity (SOPs) was presented. The proposed receiver operates in three stages: (i) Fast Fourier Transform (FFT)-based Doppler acquisition, (ii) Kalman filter (KF)-based Doppler tracking, and (iii) Doppler-compensated MULTiple SIgnal Classification (MUSIC)-based algorithm for DOA tracking. Experimental results are presented demonstrating successful tracking of the Doppler frequency and azimuth DOA of an Iridium NEXT LEO satellite, achieving a Doppler root mean square error (RMSE) of 8.1 Hz over 120 seconds and an azimuth DOA RMSE of 1.04 degrees over 60 seconds. The Doppler and azimuth DOA measurements are fused via an extended Kalman filter (EKF) to localize a stationary receiver. Starting with an initial estimate 7 km away from the true receiver’s position, the Doppler-only measurements yielded a final positioning error of 656. m, while the Doppler and azimuth DOA measurements reduced the error to 289.5 m.

Acquisition and tracking of Starlink LEO satellite signals in low SNR regime

Acquisition and tracking of Starlink low Earth orbit (LEO) satellite signals in low signal-to-noise ratio (SNR) regime was considered. Starlink’s highly dynamic downlink LEO signal model is derived, leading to coherence conditions for which the signals can be blindly tracked in low SNR regime. Next, the full-bandwidth Starlink beacon is estimated, and a time-bandwidth analysis of this beacon is presented. Finally, joint code and carrier phase Kalman filter-based loop is proposed for tracking Starlink LEO downlink signals in low SNR regime. Experimental results are presented showing successful Doppler tracking of 10 Starlink LEO satellites with a stationary receiver in low SNR regime. The Doppler observables were fused in a batch nonlinear least-squares estimator to yield a two-dimensional (2D) positioning error of 21.2 m, starting from an initial estimate 100 km away from the true position.

Evaluation of orbit errors and measurement corrections in differential navigation with LEO satellites

May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.
Ephemeris errors and measurement corrections in differential navigation with low Earth orbit (LEO) space vehicles (SVs) are analyzed. First, orbit errors are characterized for the non-differential case, showing the dependency of the range measurement errors on the receiver-to-SV geometry. The study is then extended to the differential case, where the maximum differential range error is found to occur when the baseline is normal to the projected measurement vector from one receiver onto the local navigation frame. A simulation study is presented to assess the differential navigation performance with 14 Starlink and 11 OneWeb LEO satellites. The framework fused differenced pseudorange measurements from a base and rover to LEO SVs with inertial measurement unit (IMU) measurements via an extended Kalman filter (EKF) in a tightly-coupled fashion to estimate the rover’s states. The simulation considered an aerial vehicle equipped with a tactical-grade IMU, an altimeter, a GNSS receiver, and a LEO receiver making pseudorange measurements to the LEO SVs. During 300 seconds of flight time, the vehicle traveled a distance of 28 km, the last 23 km of which were without GNSS, achieving a three-dimensional (3-D) position root mean squared error (RMSE) of 52 cm, compared to 12.5 m using the non-differential framework. Experimental results are presented, showing the potential of differential navigation in reducing ephemeris, clocks, and atmospheric errors. A ground vehicle traversed a distance of 540 m in 60 seconds, the last 492 m of which without GNSS signals, while making Doppler measurements to 2 Orbcomm and 1 Iridium LEO SVs, whose ephemerides were obtained from two-line element (TLE) files, propagated with simplified general perturbation 4 (SGP4) orbit propagator. The differential framework yielded a position RMSE of 7.13 m, compared to 41.29 m using non-differential measurements, and 87.74 m with GNSS-aided IMU.

**Blind Doppler tracking and positioning with NOAA LEO satellite signals**

A spectral approach for blind acquisition and Doppler tracking of low Earth orbit (LEO) satellite signals was applied to National Oceanic and Atmospheric Administration (NOAA) satellites. The approach accounts for the high LEO satellites’ dynamic channel, by deriving an appropriate model for the received signal frequency spectrum. A frequency-domain-based Doppler discriminator is utilized along with a Kalman filter-based Doppler tracking algorithm. Experimental results are presented showing successful acquisition and Doppler tracking of NOAA LEO satellite signals. Next, the approach is demonstrated in multi-constellation LEO acquisition and tracking, showing Hz-level Doppler tracking of 4 Starlink, 2 OneWeb, 1 Iridium NEXT, 1 Orbcomm, and 1 NOAA LEO satellites. Carrier phase observables were constructed from the tracked Doppler and fused through a nonlinear least-squares estimator to localize a stationary receiver. Starting with an initial estimate 3,600 km away from the receiver’s true position, the proposed approach is shown to achieve a two-dimensional (2D) error of 5.1 m.

**Analysis of satellite ephemeris error in differential and non-differential navigation with LEO satellites**

Low Earth orbit (LEO) satellite ephemeris error was analyzed for standalone (non-differential) and differential navigation. First, the range residual due to ephemeris error is derived for a standalone stationary receiver making range-type measurements to a LEO satellite, leading to deriving upper and lower bounds to this residual. Second, the derived residual is generalized to a differential framework, comprising two receivers making range-type measurements to the same LEO satellite. The differential range residual is found to be minimized whenever the baseline between the receivers is colinear with the projected line-of-sight (LOS) vectors on the local navigation plane, and maximized in the normal direction. Third, the combined effect of the baseline’s orientation and distance is analyzed, where the distance between the two receivers is shown to have no impact on the differential residual along the direction of...
minimum error. Finally, experimental results are presented to demonstrate the benefit of differential navigation. A ground vehicle traveled for 486 m in 50 seconds, while aiding its onboard inertial measurement unit (IMU) with differential Doppler measurements from 2 Starlink, 1 Orbcomm, and 1 Iridium LEO satellites, whose erroneous ephemerides were obtained from SGP4, initialized with two-line element (TLE) files. It is shown that differential navigation significantly reduces the effect of LEO ephemerides errors, achieving a two-dimensional (2D) position root-mean squared error (RMSE) of 11.7 m, as compared to 54.4 m for the non-differential scenario.

How have the results been disseminated?

- Prof. Zak Kassas co-organized with Dr. Dorota Grejner-Brzezinska a Special Session titled "Autonomous Navigation for Ground, Seaborne, and Airborne Vehicles" at the 2023 Institute of Navigation (ION) GNSS+ Conference, Denver, CO. The session comprised invited presentations from 5 experts and leaders from government, industry, and academia: Ms. Karen Van Dyke (U.S. Department of Transportation), Dr. Timothy Seitz (Transportation Research Center (TRC) Inc.), Dr. Eldar Rubinov (FrontierSI), Dr. Ilaria Martini (u-blox AG), and Dr. Clark Taylor (Air Force Institute of Technology).

- Prof. Kassas served as a speaker and panelist on an invited Panel on "U.S. Department of Transportation: GPS at 50, Results for Transportation and New Threats" at the 103rd Transportation Research Board (TRB) Annual Meeting, Washington, D.C. The Panel was organized by Dr. Robert Hampshire (Deputy Assistant Secretary for Research and Technology and Chief Science Officer, USDOT) and moderated by Ms. Karen Van Dyke (Director of PNT & Spectrum Management, USDOT). The invited panel comprised: LtCol Robert O. Wray (U.S. Space Force, Commander, 2d Space Operations Squadron), Ken Alexander (Chief Scientific & Technical Advisor for Satellite Navigation Systems, Federal Aviation Administration), Gregory D. Winfree (Agency Director, Texas A&M Transportation Institute), and Dana A. Goward (President, Resilient Navigation & Timing Foundation).

- Prof. Zak Kassas gave an invited presentation titled "Ad Astra: Navigation with Megaconstellation LEO Satellites" and served as a panelist in the session: "Discovering the Low Earth Orbit for PNT and Beyond" at the 2024 Munich Satellite Navigation Summit. The entire program of the Summit is composed of high-profile invited talks and panel discussions afterwards. The invited session was chaired by Roberto Prieto Cerdeira (LEO-PNT Project Manager at the European Space Agency) and speakers in the session were Patrick Shannon (Founder and CEO, TrustPoint Inc.), Francis Soualle (Airbus Defence and Space GmbH), Li Zhen (Beihang University), Masaya Murata (Japan Aerospace Exploration Agency (JAXA)), and Trevor Landon (Vice President, Satelles/Iridium).

- Prof. Zhiqiang Lin has made responsible disclosure to Tesla, Apple, and Google. The result research will be presented in 2024 IEEE Symposium on Security and Privacy in May in San Francisco CA.

- CARMEN+ supported a series of seminars at UCI (attendees totaled 225 students, researchers, and practitioners).

1. Thursday, October 26 - **ITS-Irvine Transportation Colloquium: Equity and the Future of Mobility**
2. Friday, November 3 - **Wenlong Jin - Provably Safe and Human-like Car-following Model for Automated Vehicles**
3. Friday, November 17 - **Matt Dean - Early Findings of Consumer Interest in Bi-directional & Smart EV Charging**

May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.
4. Friday, January 19 - Federico Vaca - Longitudinal Trajectories and Outcomes of Teens that Ride with Impaired Drivers & Drive Impaired

- Professor Chen’s team performed responsible security vulnerability disclosure of our project results by reaching out to the potentially-affected companies. Specifically, for P1 we have reached out to 7 LiDAR suppliers and 3 autonomous driving companies, among which 5 have replied to start internal vulnerability investigations. This work has also been covered by media:

- Prof. Yener’s team worked on two papers: “Transmitter Actions for Secure Integrated Sensing and Communication” accepted to ISIT and “Low-latency Secure Integrated Sensing and Communication with Transmitter Actions” submitted to SPAWC.

- Dr. Chandra Bhat’s research team at UT Austin has presented concepts developed for infrastructure-assisted navigation at a university-wide Good Systems Symposium poster session in March 2024, as well as the Center for Transportation Research poster session in April 2024.

- Dr. Chandra Bhat was interviewed on April 7th by Spectrum News InFocus about the role of AI in the classroom and in automated vehicle research -- https://spectruminfocus.com/section/in-focus/in-focus/2024/04/07/automated-vehicles


Describe briefly what you plan to do during the next reporting period to accomplish the goals and objectives. Project proposals from CARMEN+ PIs have been solicited and are currently under review.

Section 2: Participating & Collaborating Organizations

What organizations have been involved as partners?

Cybersecurity Vulnerability/Threat Analysis for Collaborative Sensing and Autonomy OS

- Keio University, Japan, Collaborative research
- University of Florida, USA, Collaborative research
- Toyota InfoTech Labs, USA, Collaborative research
- The University of Electro-Communications, Japan, Collaborative research

Infrastructure-Based Sensor Fusion for Tracking Connected and Autonomous Supply Chain Assets in Cyber-Compromised Environments

- Caltrans, District 8, Collaborative research

Modeling Platform for Transport Network Vulnerabilities and System Performance Analysis

- City of Irvine, Collaborative research

May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.
• DOE Vehicle Technology Office and its partners, including Argonne National Laboratory, Collaborative research

**GNSS Interference: Situational Awareness and LEO Backup**

• Spire Global and OpsGroup

**Using Infrastructure to Boost Safety in a PNT World**

• The UT Austin “Good Systems” grand challenge
• The company “Cintra” (Austin, TX)

*Have other collaborators or contacts been involved?*

**Timing-based Attacks and Mitigation for Safe HATS**

Onur Günlü, an assistant professor at Linköping University in Switzerland, was involved in both conference papers we submitted since January.

**Section 3: Outputs**

*Publications, conference papers, and presentations:*

- P. Sun and R. Jayakrishnan, “An Eco-driving Algorithm with Two-Stage Advisory Speed Limits at Signalized Intersections,” *103rd Annual Meeting of Transportation Research Board*, January 2024
- P. Sun and R. Jayakrishnan, “Link-based Control: A New Intersection Control Method with Approach Signals,” 7th Conference of Transportation Research Group of India (CTRG-2023), December 2023

*May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.*
• T. Haydon and T. E. Humphreys, “Trusted inertial terrain-aided navigation (TITAN),” *in Proceedings of the ION GNSS+ Conference, 2023* [pdf]


**Invited Presentations**


• T. E. Humphreys, September 15, 2023, “Interference Patterns,” (panel presentation) ION GNSS+ Conference, Denver, CO.

• T. E. Humphreys, September 15, 2023, “Pseudoranges from Starlink,” (panel presentation) ION GNSS+ Conference, Denver, CO.

• T. E. Humphreys, October 12, 2023, “Interference Patterns: Results from 5 years of GNSS Interference Monitoring from LEO,” Association of Old Crows.

• T. E. Humphreys, February 7, 2024, “The Final Frontier is the Next One: Low-Earth Orbit’s Geostrategic Role,” Space Cybersecurity and Resilience, University of Colorado, Colorado Springs, CO.


• T. E. Humphreys, April 12, 2024, “Electronic Warfare from an Academic Perspective,” JASON Spring Meeting, Washington, DC.

• Prof. Zak Kassas gave a Keynote Presentation at the Mega Constellation Satellite Networks for 6G Workshop at the 2023 IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Toronto, Canada, titled "Ad Astra: Navigation with Megaconstellation LEO Satellites."

• Prof. Zak Kassas gave an invited distinguished lecture at the Department of Electrical and Computer Engineering at The Ohio State University (OSU). His lecture, titled "Ad Astra: Navigation
with Megaconstellation LEO Satellites," was delivered as part of the IEEE Aerospace and Electronic Systems Society (AESS) Distinguished Lecturers Program.


- **Prof. Zak Kassas gave an invited presentation at the Workshop on Space Cybersecurity and Resilience, University of Colorado, Colorado Springs (UCCS).** This invitation-only workshop gathered experts and leaders from government, academia, and federally funded research and development centers (FFRDCs).

- **Prof. Zak Kassas gave an invited presentation and served as a panelist at the National Science Foundation (NSF) Workshop on The Convergence of Smart Sensing Systems, Applications, Analytic and Decision Making.** This invitation-only workshop brought together stakeholders with domain expertise in sensing systems as well as experts in system-theoretic areas such as signal processing, optimization, machine learning, and control theory, so they can interact and address a number of present and future challenges in smart sensing and analytics. The workshop aimed at leveraging the natural synergy between different sensing technologies, their applications, and methodologies developed in analytical areas to accelerate the development in next-generation sensing technologies and systems.

- **Prof. Zak Kassas gave an invited presentation titled "No GPS, No Problem: Exploiting Signals of Opportunity for Resilient and Accurate Autonomous Navigation in GPS-Denied Environments" at the IEEE Undergraduate Chapter at The Ohio State University.**

- **Prof. Zak Kassas gave an invited presentation titled "Ad Astra: Navigation with Megaconstellation LEO Satellites" at the Forum Munich Aerospace event "Navigation Threats and Solutions: Interference Detection and Signals of Opportunity," hosted by the Technical University of Munich (TUM).**

- **Prof. Zak Kassas gave an invited distinguished lecture at the Department of Electrical and Information Technology at Lund University, Sweden.** His lecture, titled "No GPS, No Problem: Exploiting Signals of Opportunity for Resilient and Accurate Autonomous Navigation in GPS-Denied Environments," was delivered as part of the IEEE Aerospace and Electronic Systems Society (AESS) Distinguished Lecturers Program.

- **Prof. Zak Kassas gave an invited distinguished lecture at the Department of Electrical Engineering at Chalmers University of Technology, Gothenburg, Sweden.** His lecture, titled "Ad Astra: Navigation with Megaconstellation LEO Satellites," was delivered as part of the IEEE Aerospace and Electronic Systems Society (AESS) Distinguished Lecturers Program.

**Journal publications:**


*May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.*


*Books or other non-periodical, one-time publications:*
Nothing to report.

*Other publications and presentations:*

- Y. Kwag and C. Toth, “A Review on End-to-End High-Definition Map Generation,” accepted for presentation at the *ISPRS TC I Symposium*, Las Vegas, May 11-14, 2024, and publication in the *ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences*

*Website(s) or other Internet site(s):*

**Media Reports Based on CARMEN+ Research**

- Project website for P1: [https://sites.google.com/view/cav-sec/new-gen-lidar-sec](https://sites.google.com/view/cav-sec/new-gen-lidar-sec)
- Project website for P2: [https://sites.google.com/view/cav-sec/ilr-attack](https://sites.google.com/view/cav-sec/ilr-attack)
- Project website for P3: [https://sites.google.com/view/cav-sec/roboscan](https://sites.google.com/view/cav-sec/roboscan)

*Technologies or techniques:*

**Chance-Constrained Collision Avoidance Based Motion Planning in a Cooperative Perception Framework**

Instead of using NMS as the post-processing method to remove redundant boxes, we employ Weighted-Box Fusion (WBF) to merge the detected outputs from connected vehicles. Box association was conducted using intersection-over-union (IoU) thresholding. The weights associated with each box for the fusion are determined by a function of IoU and the corresponding inverse predicted variance (uncertainty). This approach resulted in a significant improvement in the Average Precision metric.

*May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.*
Privacy-preserving Machine Learning Models for Traffic Forecasting

- **Inner Product Functional Encryption (IPFE):** This cryptographic technique has been developed to ensure the privacy and security of location data from drivers in traffic systems. IPFE enables the computation of inner products on encrypted data, allowing for secure data aggregation without revealing individual location details.

- **Deep Learning Models for Traffic Forecasting:** Advanced machine learning models incorporating Convolutional Long Short-Term Memory (Conv-LSTM) and Bidirectional Long Short-Term Memory (Bi-LSTM) modules have been designed. These models effectively analyze spatial and temporal traffic patterns to predict traffic flow with high accuracy.

**Inventions, patent applications, and/or licenses:**
Nothing to report.

**Section 4: Outcomes**

Please refer to Section 1 “What was accomplished under these goals?”

**Section 5: Impacts**

*What is the impact on the effectiveness of the transportation system?*

- The effectiveness of the transportation system has been significantly enhanced by our project, particularly in the domain of automated driving systems. Robust detection mechanisms for GPS spoofing attacks in Highly Automated Vehicles (HAVs) have been developed, resulting in a notable improvement in security and reliability. Various types of GPS spoofing attacks, such as turn-by-turn, overshoot and stop attacks, have been addressed with remarkable accuracy through the utilization of data-driven machine learning algorithms and data fusion techniques.

- Through the integration of these cutting-edge technologies, real-world scenarios can be navigated by HAVs with enhanced safety and precision. This proactive approach ensures protection against potential cyber threats while also contributing to the ongoing advancement and trustworthiness of autonomous vehicle technologies. The efforts undertaken have a far-reaching impact, promoting the seamless and efficient operation of the transportation system and laying the groundwork for a more secure and reliable automated driving experience.

- The findings from the research [S&P'24] directly impact the effectiveness of the transportation system by highlighting security risks that could potentially lead to unauthorized control of vehicle functionalities. This awareness urges improvements in vehicle security architectures, which, when implemented, could enhance the reliability and safety of transportation systems. By addressing these vulnerabilities, transportation entities can avoid potential disruptions and enhance user confidence in automated transportation technologies.

- Koti Allu’s doctoral research conducted under PI Ritchie demonstrated how augmented sensing using infrastructure-based LiDAR can enhance system manager’s understanding of Heavy-Duty truck utilization in both rural and urban areas along with their impacts on transportation.

- The transportation system's future is expected to be significantly impacted by developing a sophisticated MAS framework and integrating cooperative control strategies and collision avoidance algorithms. Through the efficient management of traffic flow and the possibility of conflict mitigation, it is anticipated to improve safety, efficiency, and dependability in urban...
contexts. This development may result in fewer accidents, less congestion, and more efficient traffic operations, all of which could pave the way for future travel that is safer and more seamless.

- **Enhanced Traffic Prediction Accuracy**: The hybrid deep learning models developed, which incorporate Conv-LSTM and Bi-LSTM techniques infused with a Squeeze-and-Excitation (SE) module, have been implemented to predict traffic flow patterns more accurately. This would lead to improved traffic management and congestion mitigation, evidenced by the overall reduced mean absolute error rates in traffic forecasts. The precise traffic forecasting enables proactive management strategies, enhancing overall transportation system efficiency.

- **Privacy Preservation in Data Collection**: The application of Inner Product Functional Encryption (IPFE) will enable secure and private data aggregation from numerous traffic sensors without compromising individual data privacy. This approach fosters wider adoption of data-driven traffic management practices while adhering to privacy regulations, thereby increasing the trust and reliability of transportation data systems.

- **Operational Improvements and Policy Development**: The research findings would support the development of new policies focusing on data security and privacy in ITS (Intelligent Transportation Systems). Thereby leading to operational improvements within traffic management centers, with better compliance with data protection laws and enhanced decision-making capabilities.

**What is the impact of technology transfer on industry and government entities, on the adoption of new practices, or on research outcomes which have led to initiating a start-up company?**


**What is the impact on the body of scientific knowledge?**

- Please refer to the publications section.

**What is the impact on transportation workforce development?**

In this reporting period, we are able to make impacts on transportation workforce development by (1) providing research opportunities for 3 PhD students and 2 undergraduate students at UCI; (2) providing new educational materials for the transportation security lecture in the graduate-level security course Co-PI Chen is teaching annually; (3) improving the performance, skills, or aptitudes of members of underrepresented groups, for example for a female UCI PhD student Fayzah Alshammari to have the opportunity to work on transportation research topics; and (4) providing opportunity for Co-PI Chen to achieve continuity in leading the organization of the second ISOC Symposium on Vehicle Security and Privacy (VehicleSec) in Feb 2024, which is the first official academic conference dedicated to vehicle
security and privacy topics (co-founded by Co-PI Chen in 2023). This can directly facilitate the transportation workforce development by providing/creating more professional opportunities for students, researchers, and practitioners on transportation security topics.

The program will have notable impact on transportation workforce development in several key areas:

- **Research and Teaching Opportunities**: The program will provide significant opportunities for research and teaching in transportation and related disciplines. By developing new technologies and methodologies, like an advanced privacy-preserving traffic forecasting system, the program will enrich academic curricula and research activities. These initiatives will help to integrate cutting-edge scientific knowledge into transportation studies, thereby fostering a deeper understanding and interest in this field among students and researchers.

- **Enhancing Skills of Underrepresented Groups**: The program will help improving the performance, skills, and aptitudes of members of underrepresented groups. By involving these groups in research projects and offering targeted training programs, to enhance their technical capabilities and professional opportunities in transportation research, teaching, or related professions. This effort helps in improving access to and retention of these groups in the transportation sector, contributing to a more diverse and inclusive workforce.

**Section 6: Changes/Problems**

*Changes in approach and reasons for change*
Nothing to report.

*Actual or anticipated problems or delays and actions or plans to resolve them*
Nothing to report.

*Changes that have a significant impact on expenditures*
Nothing to report.

*Significant changes in use or care of human subjects, vertebrate animals, and/or biohazards*
Nothing to report.

*Change of primary performance site location from that originally proposed*
Nothing to report.

**Section 7: Special Reporting Requirements**

Nothing to report.

**Section 8: Performance Indicators**

- Prof. Zak Kassas was appointed a Senior Editor for the IEEE Transactions on Intelligent Transportation Systems.
- The paper by Haitham Kanj, Sharbel Kozhaya, and Prof. Kassas, titled "Acquisition and tracking of Starlink LEO satellite signals in low SNR regime" won the Best Paper Presentation award in the...


- CARMEN UTC alumnus Dr. Mohammad Neinavaie received the 2023 Dr. Robert Dybdal ElectroScience Laboratory Best Ph.D. Dissertation Award for his Ph.D. Dissertation titled "Cognitive sensing and navigation with unknown terrestrial and LEO satellite signals." ESL is a center-of-excellence lab focusing on radio frequency (RF), optics, and electromagnetic research. Since 1942, ESL has consistently maintained a national and international preeminence in electromagnetics and RF systems. ESL is the home to more than 100 graduate and undergraduate students, and through the years, more than 1,000 PhD and master's students graduated from ESL and gone on to successful careers in government, industry, and academia.

- Prof. Kassas was elected Fellow of the IEEE) The number of IEEE Fellows elevated in a year is no more than one-tenth of one percent of the total IEEE voting membership. Prof. Kassas was elected for "contributions to navigation with signals of opportunity."

- Prof. Kassas, his students (Dr. Joe Khalife and Dr. Ali Abdallah), and Mr. Chiawei Lee (Director of Research, US Air Force Test Pilot School) won the 2022 IEEE Aerospace and Electronic Systems Society (AESS) Harry Rowe Mimno Award for their paper titled “I Am Not Afraid of the GPS Jammer: Resilient Navigation Via Signals of Opportunity in GPS-Denied Environments.” Established in 1979, this annual award is given in recognition of the best paper published in the peer-reviewed IEEE Aerospace and Electronic Systems Magazine. The award is given two-years after papers get published (to allow for some time to pass to measure the paper's impact).

- A member of Dr. Bhat’s team, PhD student Angela Haddad, received the Women in Transportation Seminar (WTS) Heart of Texas Chapter award based on her contributions to research and leadership, including her activities related to the CARMEN+ grant.

- Dr. Bhat is ranked as one of the top three scientists globally in the combined field of Logistics and Transportation based on Scopus and other sources, as extracted from Ioannidis, John P.A. (2023), “October 2023 data-update for "Updated science-wide author databases of standardized citation indicators", Elsevier Data Repository, V6, doi: 10.17632/btchxktzyw.6, (https://elsevier.digitalcommonsdata.com/datasets/btchxktzyw/6).