NATIONAL CENTER FOR TRANSPORTATION CYBERSECURITY AND RESILIENCY
*A USDOT National Transportation Center*

| | |
|---|---|
| **Project Title:** | Multimodal In-Vehicle Sensor Fusion for Cyber-Secured Autonomous Navigation |
| **PI Name and Contact:** | Mizanur Rahman, Ph.D.<br>Assistant Professor<br>Department of Civil, Construction & Environmental Engineering<br>2007 Smart Communities and Innovation Building (SCIB)<br>The University of Alabama, Tuscaloosa, AL 35487<br>Phone: (205) 348-1717<br>Email: mizan.rahman@ua.edu |
| **Submission Date:** | February 10, 2025 |
| **Version:** | 1.0 |
| **Project Performance Period** | January 1, 2024 – December 31, 2024 |

## Project Summary

The security and reliability of Global Navigation Satellite Systems (GNSS) are critical for the safe operation of autonomous vehicles (AVs). However, GNSS signals are vulnerable to spoofing attacks, which can mislead AV navigation systems and compromise operational safety. This report addresses this vulnerability by developing detection and mitigation against GNSS spoofing attacks, with a particular focus on a slow drift GNSS spoofing attack. The study first investigates slow drift GNSS spoofing attacks, a stealthy form of signal manipulation where the attack gradually shifts the perceived position of the AV without triggering traditional anomaly detection mechanisms. To counteract this type of attack, a multi-sensor fusion-based spoofing detection framework is presented, integrating data from in-vehicle sensors, including speedometers, accelerometers, and gyroscope sensors, to cross-validate GNSS-derived positioning. The framework utilizes Long Short-Term Memory (LSTM) neural networks to predict vehicle motion and detect inconsistencies indicative of spoofing attacks. Field experiments validate the framework's effectiveness, achieving a 97.3% accuracy in identifying spoofing scenarios while maintaining a low false positive rate. Additionally, a Geographical Information Systems (GIS) and landmark-based navigation approach is developed for AV localization in GNSS-contested environments. This approach leverages in-vehicle sensor data, 2D map, and urban landmarks, such as roadway intersection, to provide an alternative positioning method. LSTM and Kalman Filters are utilized to enhance location shift prediction and position correction. The results of this research underscore the necessity of integrating multi-sensor validation and GIS-assisted navigation into AV systems to mitigate GNSS spoofing threats. The approaches could contribute to the development of cyber-resilient AV navigation frameworks, enhancing security in urban and contested environments in the presence of GNSS spoofing threats.

## 1. Data Description

Reports and data produced as part of this project are expected to include, but are not limited to, websites, publications, and archival-quality data curated from various sources. These reports will include technical documents with detailed figures, such as tables, graphs, and scripts essential for analyzing and interpreting the data. The project will generate structured datasets and programming data. The structured datasets will include GNSS signal data collected from the live sky (legitimate signals). Additional datasets will include multimodal sensor data from IMU and cameras. These data will also incorporate vehicle dynamics information, such as velocity, acceleration, and route geometry. Programming data will consist of algorithms and scripts developed in MATLAB, Python, and Java for threat modeling, spoofing detection, trustworthy monitoring modules, and cyber-resilient navigation frameworks.

## 2. Data format and metadata standards

Detailed data will be documented corresponding to each metadata set available in at least one of the following formats: XML, CSV, plain text, PDF, HTML, MS Word, or LaTeX. The aggregated data will be in plain text format and may be compressed for space-saving purposes. Programming scripts will be maintained in MATLAB, Python, and Java formats. GNSS signal data, including live sky and simulated spoofed signals, will be saved in binary formats compatible with processing tools. Comprehensive metadata will accompany all datasets, including descriptions of variables, data collection procedures, and processing methods. Data dictionaries will be provided for all the related data, and standards used for data and metadata format and content will be documented with proposed solutions and remedies. Metadata and data standards will align with the DCAT-US Schema v1.1 to support interoperability and compliance with federal data repositories like the USDOT Research Data Exchange (RDE). The data files will be stored and backed up in UA+BOX provided by the University

of Alabama (UA). UA+Box provides a secure, managed, cloud-based toolset, and storage to facilitate collaboration and anywhere-access to active files and data. All data are encrypted both in transit and storage and are maintained on domestic servers. This storage is provided to UA faculty without charge.

## 3. Access Policies

Access to, sharing, and distributing documentation will be via websites, as well as publishing and presenting in conferences, journals, and monographs. As per request, the data will be shared via the TraCR website and USDOT Repository & Open Science Access Portal enabling the research community to access and reproduce research activities. Due to privacy and sensitivity, the identification data from camera videos, as well as sensor data, will be desensitized for open use. All sensitive personal information in the data will be removed. The Principal Investigator (PI) will coordinate with the associate directors and TraCR's director to oversee data management. Access to the raw data stored in UA+Box will require approval from the PI to ensure security and compliance. The reports produced from this project will be maintained and made available by TraCR.

## 4. Policies and Provisions for Re-use, Redistribution, derivatives

The author(s) and the researcher(s) reserve all rights to intellectual property. To avoid ethical issues, sensitive personal information will be removed from the datasets before they are shared. Should any third-party data be used, proper attribution will be provided, and licensing requirements will be strictly adhered to.

## 5. Plans for Archiving and Preservation of Access and Data Integrity

Long-term data includes GNSS signal data (live sky and simulated spoofed signals), multimodal sensor data, metadata, programming scripts, and project reports. The long-term strategy for maintaining, curating, and archiving the data is to seek support from the UA Office of Information (OIT). The OIT datacenter operates an enterprise-class Compellent SAN storage platform with daily replication/replay to a backup Compellent SAN located in our Atlanta Continuity of Operations facility, which is a highly secured Tier 2 disaster recovery facility. PI will ask the OIT data center to archive the data from this project for ten years.

## 6. Change Log

| Version | Date | Description |
|---|---|---|
| 1.0 | Jan 23, 2025 | Initial submission of the Data Management Plan. |